ESET Smart Security 4
使用者手冊

Microsoft® Windows® 7 / Vista / XP / 2000 / 2003 / 2008

we protect your digital worlds

ESET Smart Security 4

Copyright © 2009 by ESET, spol. s. r. o.

ESET Smart Security 4 由 ESET, spol. s r.o. 開發。
如需相關資料，請造訪 www.eset.com。
保留所有權利。未經作者書面許可，不得以任何形式重製、儲存於檢索系統或轉錄本出版品的任何內容，或透過任何手段進行電子發送、機械處理、複製照片、記錄、掃描等。
ESET, spol. s r.o. 保留變更任何提及之應用程式軟體而不先行通知的權力。

全球客戶服務：www.eset.eu/support
北美客戶服務：www.eset.com/support

REV.20081107-006

目錄

1. ESET Smart Security 4 4

1.1 新增功能 4
1.2 系統需求 5

2. 安裝 6

2.1 一般安裝 6
2.2 自訂安裝 7
2.3 使用原始設定 9
2.4 輸入使用者名稱及密碼 9
2.5 手動電腦掃描 9

3. 初學者手冊 10

3.1 介紹使用者介面設計 – 模式 10
3.1.1 檢查系統的作業 10
3.1.2 如果程式運作不正常怎麼辦 10
3.2 更新設定 11
3.3 受信任區域設定 11
3.4 Proxy 伺服器設定 12
3.5 設定保護 12

4. 使用 ESET Smart Security 13

4.1 病毒及間諜程式防護 13
4.1.1 即時檔案系統防護 13
4.1.1.1 控制項設定 13
4.1.1.1.1 要掃描的媒體 13
4.1.1.1.2 執行掃描的時間（事件觸發的掃描） 13
4.1.1.1.3 用於新建立及已修改檔案的其他 ThreatSense 參數 13
4.1.1.1.4 進階設定 13
4.1.1.2 清除層級 13
4.1.1.3 何時修改即時保護設定 13
4.1.1.4 檢查即時防護 13
4.1.1.5 即時防護無法運作時怎麼辦 14
4.1.2 電子郵件用戶端防護 14
4.1.2.1 POP3 檢查 14
4.1.2.1.1 相容性 14
4.1.2.2 與電子郵件用戶端整合 15
4.1.2.2.1 將標籤訊息附加到電子郵件內容 15
4.1.2.3 移除入侵 15
4.1.3 Web 存取防護 15
4.1.3.1 HTTP、HTTPS 15
4.1.3.1.1 位址管理 16
4.1.3.1.2 Web 瀏覽器 16
4.1.4 電腦掃描 16
4.1.4.1 掃描類型 16
4.1.4.1.1 標準掃描 16
4.1.4.1.2 自訂掃描 17
4.1.4.2 掃描目標 17
4.1.4.3 掃描設定檔 17
4.1.5 通訊協定篩選 17
4.1.5.1 SSL 17

4.1.5.1.1 可信任的憑證 18
4.1.5.1.2 排除的憑證 18
4.1.6 ThreatSense 引擎參數設定 18
4.1.6.1 物件設定 18
4.1.6.2 選項 18
4.1.6.3 清除 19
4.1.6.4 副檔名 19
4.1.6.5 限制 19
4.1.6.6 其他 19
4.1.7 偵測到入侵 19

4.2 個人防火牆 20
4.2.1 過濾模式 20
4.2.2 封鎖所有流量：中斷網路 20
4.2.3 停用過濾：允許所有連線 20
4.2.4 配置及使用規則 20
4.2.4.1 建立新規則 21
4.2.4.2 編輯規則 21
4.2.5 配置區域 21
4.2.6 建立連線 - 偵測 22
4.2.7 記錄 22

4.3 垃圾郵件防護 22
4.3.1 自學垃圾郵件防護 23
4.3.1.1 新增位址到白名單 23
4.3.1.2 將郵件標記為垃圾郵件 23

4.4 更新程式 23
4.4.1 更新設定 23
4.4.1.1 更新設定檔 24
4.4.1.2 進階更新設定 24
4.4.1.2.1 更新模式 24
4.4.1.2.2 Proxy 伺服器 24
4.4.1.2.3 連線至 LAN 25
4.4.1.2.4 建立更新副本 – 映像 25
4.4.1.2.4.1 從映像更新 26
4.4.1.2.4.2 疑難排解映像更新問題 26
4.4.2 如何建立更新工作 26

4.5 工作安排精靈 27
4.5.1 排定工作的目的 27
4.5.2 建立新工作 27

4.6 隔離 28
4.6.1 隔離檔案 28
4.6.2 從隔離區還原 28
4.6.3 從隔離區提交檔案 28

4.7 防護記錄檔案 28
4.7.1 防護記錄維護 29

4.8 使用者介面 29
4.8.1 警告及通知 29

4.9 ThreatSense.Net 30
4.9.1 可疑檔案 30
4.9.2 統計資料 31
4.9.3 提交 31

4.10 遠端管理 31

4.11 授權 32

5. 進階使用者 33

5.1 Proxy 伺服器設定 33

5.2 匯出/匯入設定 33
5.2.1 匯出設定 33
5.2.2 匯入設定 33

5.3 指令列 33

5.4 ESET SysInspector 34
5.4.1 使用者介面與應用程式使用 34
5.4.1.1 程式控制 34
5.4.1.2 瀏覽 ESET SysInspector 35
5.4.1.3 比較 35
5.4.1.4 ESET Smart Security 4 中的 SysInspector 36

5.5 ESET SysRescue 36
5.5.1 最低需求 36
5.5.2 如何建立救援 CD 36
5.5.2.1 資料夾 36
5.5.2.2 ESET 病毒防護 36
5.5.2.3 進階 36
5.5.2.4 可開機 USB 裝置 36
5.5.2.5 燒錄 37
5.5.3 使用 ESET SysRescue 37
5.5.3.1 使用 ESET SysRescue 37

6. 詞彙 38

6.1 入侵類型 38
6.1.1 病毒 38
6.1.2 蠕蟲 38
6.1.3 特洛伊木馬程式 38
6.1.4 Rootkit 38
6.1.5 廣告程式 38
6.1.6 間諜程式 38
6.1.7 有潛在危險的程式 39
6.1.8 潛在不需要應用程式 39

6.2 遠端攻擊的類型 39
6.2.1 DoS 攻擊 39
6.2.2 DNS Poisoning 39
6.2.3 蠕蟲攻擊 39
6.2.4 通訊埠掃描 39
6.2.5 TCP 去同步化 39
6.2.6 SMB Relay 39
6.2.7 ICMP 攻擊 39

6.3 電子郵件 39
6.3.1 廣告 40
6.3.2 惡作劇 40
6.3.3 網路釣魚 40
6.3.4 識別垃圾郵件詐騙 40
6.3.4.1 規則 40
6.3.4.2 貝氏過濾 40
6.3.4.3 白名單 40
6.3.4.4 黑名單 40
6.3.4.5 伺服器端控制 40

1. ESET Smart Security 4

ESET Smart Security 4 首先採用創新的方式，提供真正的整合式電腦安全性。本產品運用 ESET NOD32 Antivirus 的速度及準確度（有最新版 ThreatSense® 掃描引擎的品質保證），結合量身訂做的「個人防火牆」及「垃圾郵件防護」模組。打造出隨時保持警戒的智慧型系統，為您防護會危害電腦的攻擊和惡意軟體。

ESET Smart Security 不像其他廠商，只是將不同產品組合成笨重的大型程式。這是長期努力的結果，讓系統在佔用最低使用量的情況下獲得最大保護。這些以人工智慧為基礎的先進技術，能夠在不妨礙系統效能或不中斷系統的情況下，主動消除病毒、間諜軟體、特洛伊木馬程式、蠕蟲、廣告軟體、Rootkit 及網際網路所產生其他攻擊的侵入。

1.1 新增功能

我們專家長期累積下來的開發經驗，造就全新架構的 ESET Smart Security 程式，確保能以最少系統需求提供最強的偵測能力。複雜的安全性解決方案包含具有數種進階選項的模組。下列清單提供您這些模組的概觀。

- **病毒及間諜程式防護**

此模組以 ThreatSense® 掃描核心為基礎，此掃描核心最初用於獲獎的 NOD 32 Antivirus 系統上。ThreatSense® 核心在最新的 ESET Smart Security 架構下，已經最佳化及改良。

功能	説明
改良的清除功能	目前，防毒系統已能在無須使用者介入的情況下，智慧型地清除與刪除所偵測到的大部分入侵活動。
背景掃描模式	可在背景啟動電腦掃描，而不會減緩效能。
更小的更新檔案	核心最佳化處理程序會讓更新檔案的大小保持小於 2,7 版的大小。此外，也改善了保護更新檔案不致損毀的能力。
提供常用電子郵件用戶端的防護	本產品現在不但可以掃描 MS Outlook 中的對內郵件，也能夠掃描 Outlook Express、Windows Mail、Windows Live Mail 及 Mozilla Thunderbird 中的對內郵件。
各種其他次要改進功能	– 直接存取檔案系統，以提升速度及輸送量。 – 封鎖受感染檔案的存取 – 為 Windows Security Center 進行最佳化，包括 Vista。

- **個人防火牆**

「個人防火牆」會監視受保護電腦與網路中其他電腦之間的所有流量。「ESET 個人防火牆」包含各種先進功能，列示如下。

功能	説明
低層網路通訊掃描	「資料連結層」上的網路通訊掃描可讓「ESET 個人防火牆」克服各種本來無法偵測的攻擊。
IPv6 支援	「ESET 個人防火牆」會顯示 IPv6 位址，並可讓使用者為其建立規則。
執行檔監視	監視執行檔中的變化，以避免感染。可修改已簽署的應用程式檔案。
與 HTTP 及 POP3 整合的檔案掃描	已將檔案掃描整合至 HTTP 及 POP3 應用程式通訊協定。使用者在瀏覽網際網路或下載電子郵件時，都能受到保護。
入侵偵測系統	能夠辨識網路通訊的特性，以及各種類型的網路攻擊，並可選擇自動禁止這類通訊。
互動、規則、學習、自動及發生例外的自動模式支援	使用者可以選擇是否要自動執行防火牆處理方法，或是要以互動方式來設定規則。規則模式中的通訊會依據使用者或網路系統管理員預先定義的規則來處理。「學習」模式會自動建立並儲存規則，適用於防火牆的起始設定。
取代整合式 Windows 防火牆	取代整合式 Windows 防火牆，它也會與 Windows Security Center 互動，所以使用者可以隨時掌握其安全性狀態。依預設，ESET Smart Security 安裝會關閉 Windows 防火牆。

- **垃圾郵件防護**

ESET 垃圾郵件防護會過濾來路不明的電子郵件，進而增加電子通訊的安全性及舒適性。

功能	説明
對內郵件評分	所有「對內」郵件都會被評分，範圍從 0（郵件為非垃圾郵件）到 100（郵件為垃圾郵件），並分別移至 [垃圾郵件] 資料夾或使用者建立的自訂資料夾。多封對內電子郵件可並行掃描。
支援各種掃描技術	- Bayes 分析 - 規則型掃描 - 全域指紋資料庫檢查
與電子郵件用戶端完全整合	垃圾郵件防護適用於 Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 及 Mozilla Thunderbird 用戶端的使用者。
可使用手動垃圾郵件選取功能	可選擇手動將電子郵件選取 / 取消選取為垃圾郵件。

- **其他**

功能	説明
ESET SysRescue	ESET SysRescue 可讓使用者建立開機 CD/DVD/USB，其中包含能夠獨立於作業系統執行的 ESET Smart Security。此功能最適合用於刪除系統難以移除的入侵。
ESET SysInspector	ESET SysInspector 這套應用程式會徹底地檢查電腦，現在已直接整合至 ESET Smart Security 中。如果您使用 [説明及支援 > 客戶關懷支援要求 (建議)] 選項聯絡「客戶關懷服務」，可選擇一併提供電腦的 ESET SysInspector 狀態快照。
文件防護	[文件防護] 會在 Microsoft Office 文件開啟之前掃描文件，並掃描 Internet Explorer 自動下載的檔案，例如 Microsoft ActiveX 元素。
自我防護	新的「自我防護」技術會防止嘗試停用 ESET Smart Security 元件。
使用者介面	目前亦可使用鍵盤控制 ESET Smart Security，以非圖形使用者介面模式運作。 並增加螢幕閱讀應用程式的相容性，讓視覺障礙者更有效地控制程式。

1.2 系統需求

為使 ESET Smart Security 及 ESET Smart Security Business Edition 作業順暢，系統應符合下列軟硬體需求：

ESET Smart Security：

Windows 2000、XP	400 MHz 32 位元 / 64 位元 (x86 / x64) 128 MB RAM 的系統記憶體 130 MB 的可用空間 Super VGA (800 × 600)
Windows 7、Vista	1 GHz 32 位元 / 64 位元 (x86 / x64) 512 MB RAM 的系統記憶體 130 MB 的可用空間 Super VGA (800 × 600)

ESET Smart Security Business Edition：

Windows 2000、2000 Server、XP、2003 Server	400 MHz 32 位元 / 64 位元 (x86 / x64) 128 MB RAM 的系統記憶體 130 MB 的可用空間 Super VGA (800 × 600)
Windows 7、Vista、Windows Server 2008	1 GHz 32 位元 / 64 位元 (x86 / x64) 512 MB RAM 的系統記憶體 130 MB 的可用空間 Super VGA (800 × 600)

2. 安裝

購買之後，您可以從 ESET 的網站下載 ESET Smart Security 安裝程式。這會是 ess_nt**_***.msi (ESET Smart Security) 或 essbe_nt**_***.msi (ESET Smart Security Business Edition) 套件。啟動安裝程式，安裝精靈將引導您進行基本設定。有兩種可用的安裝類型，其層級設定不同，詳細資訊如下：

1. 一般安裝

2. 自訂安裝

2.1 一般安裝

建議要安裝具有預設值的 ESET Smart Security 的使用者使用 [一般] 安裝。程式的預設值提供最大層級的防護，對於不想配置詳細設定的使用者而言，是最佳選擇。

第一步（最重要的一步）是輸入使用者名稱及密碼，以自動更新程式。這樣可為系統提供持續防護，是非常重要的步驟。

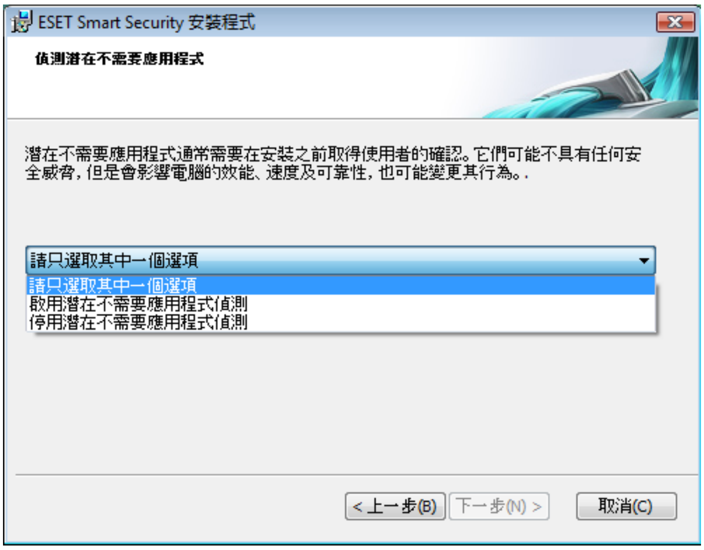
將 [**使用者名稱**] 及 [**密碼**] (如購買或註冊產品後收到的身份認證) 輸入到對應的欄位中。如果目前沒有 [使用者名稱] 及 [密碼]，請選取 [**稍後再設定更新參數**] 選項。稍後可隨時從程式直接插入身份認證。

安裝的下一步是設定「ThreatSense.Net 預早警告系統」。「ThreatSense.Net 預早警告系統」有助於確保迅速持續地通知 ESET 新入侵的相關資訊，以快速保護其客戶。系統會接受提交到 ESET 病毒實驗室的新威脅，並對其進行分析、處理及新增到病毒資料庫。

依預設會選取 [**啟用 ThreatSense.Net 預早警告系統**] 核取方塊，以啟動此功能。按一下 [**進階設定...**]，以修改提交可疑檔案的詳細設定。

安裝程序的下一步是設定 [**偵測潛在不需要應用程式**]。潛在不需要應用程式不一定是惡意的，但是可能會經常對作業系統的行為造成負面影響。

這些應用程式通常隨附於其他程式，且可能在安裝期間很難注意到。雖然這些應用程式通常會在安裝期間顯示通知，但亦可未經您的同意輕易安裝。



選取 [**啟用潛在不需要應用程式偵測**] 選項，以允許 ESET Smart Security 偵測此類型的威脅 (建議)。

[一般] 安裝模式中的最後一步是按一下 [**安裝**] 按鈕，確認安裝。

2.2 自訂安裝

[**自訂**] 安裝的目標使用者，是具有微調程式經驗，並希望在安裝期間修改進階設定者。

第一步驟是選取安裝的目標位置。依預設，程式會安裝到 C:\Program Files\ESET\ESET Smart Security\。按一下 [**瀏覽…**] 以變更此位置 (不建議)。

第二步驟是 [**輸入使用者名稱及密碼**]。此步驟與 [一般] 安裝相同 (請參閱第 5 頁)。

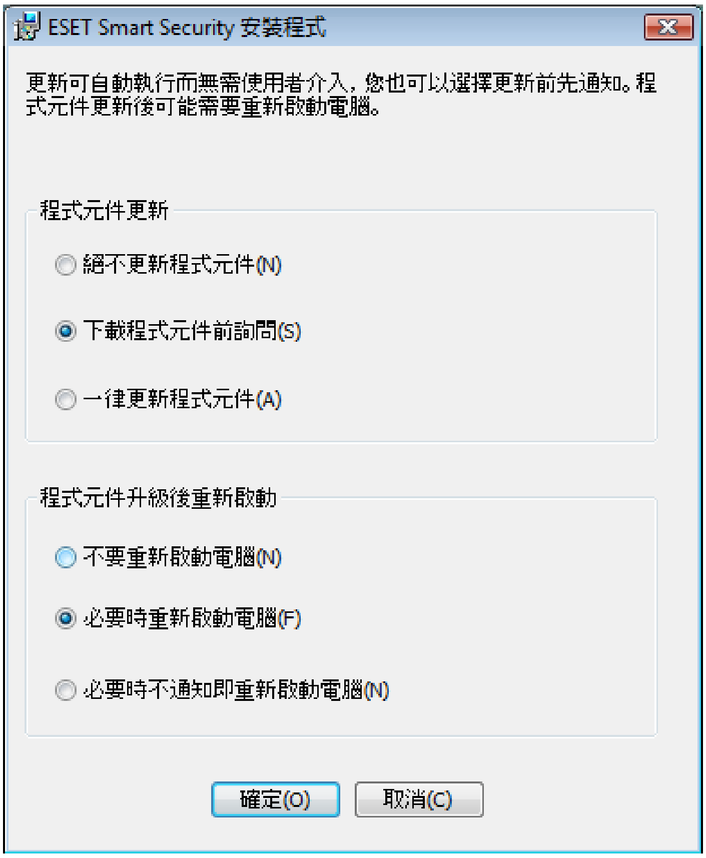
在輸入您的 [使用者名稱] 及 [密碼] 之後，按 [**下一步**] 以 [**配置您的網際網路連線**]。

如果您使用 Proxy 伺服器，則必須正確設定，才能讓病毒資料庫更新正常運作。如果您不知道是否是使用 Proxy 伺服器連接至網際網路，則保留預設值 [**我不確定我的網際網路連線是否使用 Proxy 伺服器。請使用與 Internet Explorer 相同的設定**]，並按 [**下一步**]。如果您未使用 Proxy 伺服器，請選取對應選項。

若要設定您的 Proxy 伺服器設定，請選取 [**我使用 Proxy 伺服器**]，並按 [**下一步**]。將 Proxy 伺服器的 IP 位址或 URL 輸入到 [**位址**] 欄位中。在 [**連接埠**] 欄位中，指定 Proxy 伺服器接受連線所在的連接埠 (依預設為 3128)。如果 Proxy 伺服器需要驗證，則必須輸入有效的使用者名稱及密碼，授與 Proxy 伺服器的存取權限。如果需要，也可以從 Internet Explorer 複製 Proxy 伺服器設定。若要這樣做，請按一下 [**套用**] 並確認選項。

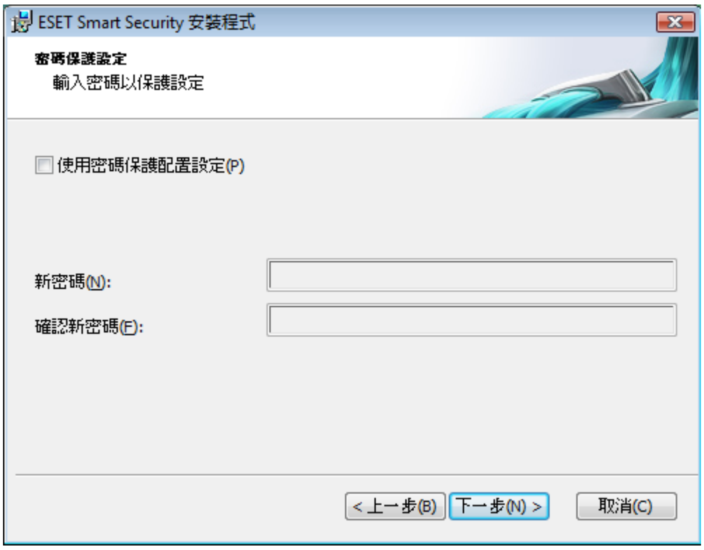
按 [**下一步**] 繼續前往 [**配置自動更新設定**] 視窗。此步驟可讓您指定系統上處理自動程式元件更新的方式。按一下 [**變更...**] 以存取進階設定。

如果您不想要更新程式元件，請選取 [**絕不更新程式元件**]。啟用 [**下載程式元件前詢問**] 選項，則會在下載程式元件之前顯示確認視窗。若要啟用無提示的自動程式元件升級，請選取 [**執行程式元件升級 (若有的話)**] 選項。



附註：程式元件升級之後，通常需要重新開機。建議的設定為：**必要時不通知即重新啟動電腦**。

安裝的下一步是「輸入密碼」以保護程式參數。選擇要用於保護程式的密碼。重新輸入密碼進行確認。



[**配置 ThreatSense.Net 預早警告系統**] 及 [**偵測潛在不需要應用程式**] 步驟與 [一般] 安裝相同，且不在此處顯示 (請參閱第 5 頁)。

[自訂] 模式中的最後一步是選取「ESET 個人防火牆」過濾模式。共有五種可用的模式：

- 自動
- 發生例外情況的自動模式 (使用者定義的規則)
- 互動
- 規則
- 學習

建議大部分使用者使用 [**自動**] 模式。這樣會啟用所有標準對外連線 (使用預先定義的設定自動分析)，且自動封鎖來路不明的對內連線。

發生例外的自動模式 (使用者定義的規則)。除了自動模式之外，還可讓您新增自訂規則。

[**互動**] 模式適用於進階使用者。通訊由使用者定義的規則處理。如果沒有定義任何通訊規則，則程式會要求使用者允許或拒絕通訊。

[**規則**]　模式會根據管理員建立的預先定義規則評估通訊。如果沒有可用規則，則會自動封鎖連線，使用者不會看到任何警告訊息。建議唯有設定網路通訊的系統管理員，才選用規則模式。

學習模式 - 自動建立及儲存規則，適用於個人防火牆的起始配置。此模式不需要使用者互動，因為 ESET Smart Security 會根據預先定義的參數儲存規則。[學習] 模式並不安全，請僅於已針對必要的通訊建立所有規則時才使用。

最後一個步驟會顯示視窗，要求您確認進行安裝。

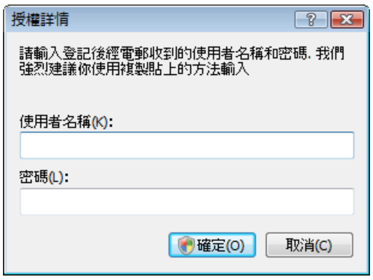
2.3 使用原始設定

如果您重新安裝 ESET Smart Security，則會顯示 [**使用現有的設定**] 選項。選取此選項，將設定參數從原始安裝傳輸至新的安裝。

2.4 輸入使用者名稱及密碼

為取得最佳功能，請務必自動更新程式。唯有更新設定中輸入正確的使用者名稱及密碼，才能達到此目的。

如果安裝期間未輸入使用者名稱及密碼，現在可以輸入。在主要程式視窗中，按一下 [**更新**]，然後按一下 [**使用者名稱及密碼設定...**]。將接收到的資料及產品授權輸入 [**授權詳情**] 視窗中。



2.5 手動電腦掃描

安裝 ESET Smart Security 之後，應執行電腦掃描，檢查是否有惡意代碼。若要快速啟動掃描，請從主要功能表中選取 [**電腦掃描**]，然後在主要程式視窗中選取 [**標準掃描**]。如需「電腦掃描」功能的相關資訊，請參閱「電腦掃描」一章。

3. 初學者手冊

本章提供 ESET Smart Security 及其基本設定的初始概觀。

3.1 介紹使用者介面設計 – 模式

ESET Smart Security 的主視窗分為兩個主要區段 左側直欄可存取簡單易用的主要功能表。右側的主要程式視窗主要顯示與主要功能表中所選選項相對應的資訊。

以下為主要功能表中按鈕的說明：

防護狀態 - 以簡單易用的形式，提供 ESET Smart Security 防護狀態的相關資訊。如果啟動［進階］模式，則會顯示所有防護模組的狀態。按一下模組以檢視其目前狀態。

電腦掃描 - 此選項可讓使用者設定及啟動 [手動電腦掃描]。

更新 - 選取此選項以存取管理病毒資料庫更新的更新模組。

設定 - 選取此選項以調整您電腦的安全等級。如果啟動「進階」模式，則會顯示 [病毒及間諜程式防護]、[個人防火牆] 及 [垃圾郵件防護模組] 子功能表。

工具 - 此選項僅在 [進階] 模式中可用。可在此存取「防護記錄檔案」、「隔離」及「工作安排精靈」。

說明及支援 - 選取此選項以存取說明檔、「ESET 知識庫」、ESET 的網站，以及「客戶關懷」支援要求。

ESET Smart Security 使用者介面可讓使用者切換 [標準] 及 [進階] 模式。若要在模式之間切換，請參閱位於主要 ESET Smart Security 視窗左下角的 **[顯示]** 連結。按一下此按鈕以選取需要的顯示模式。

[標準] 模式可存取一般作業所需的功能。不顯示任何進階選項。

切換至 [進階] 模式會將 **[工具]** 選項新增至主要功能表。[工具] 選項可讓使用者存取「排程器」、「隔離區」或檢視 ESET Smart Security 防護記錄檔案。

附註：本手冊中以下的所有說明，均針對 [進階] 模式。

3.1.1 檢查系統的作業

若要檢視［**防護狀態**］，請按一下主要功能表頂端的這個選項。ESET Smart Security 的作業狀態摘要會顯示在視窗的右側，並顯示具有三個項目的子功能表：**防毒與反間諜軟體**、**個人防火牆**及**垃圾郵件防護模組**。選取以上任一選項，以檢視特定保護模組的更多詳細資訊。

如果啟用的模組正常運作，則會標上綠色核取記號。如果不正常，則會顯示紅色驚嘆號或橙色通知圖示，且視窗的上半部會顯示模組的其他相關資訊。同時還會顯示修正模組的建議解決方案。若要變更個別模組的狀態，請按一下主要功能表中的 **[設定]**，並按一下需要的模組。

3.1.2 如果程式運作不正常怎麼辦

如果 ESET Smart Security 在任何防護模組中偵測到問題，則會在 **[防護狀態]** 視窗中報告。此處還會提供問題可能的解決方案。

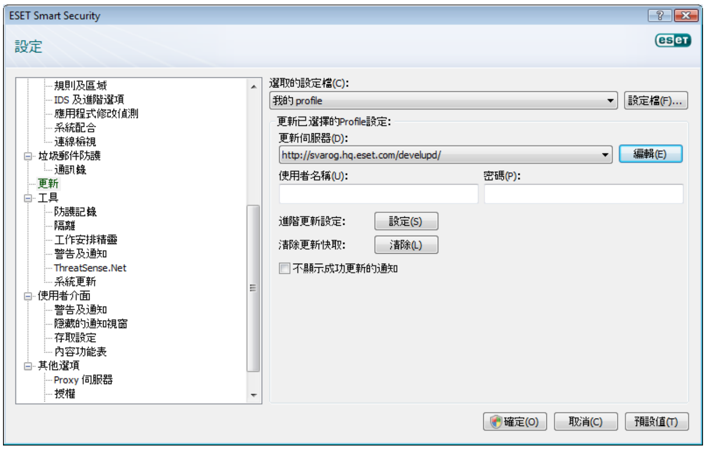
如果無法透過使用所顯示的已知問題及解決方案清單解決問題，請按一下 **[說明及支援]** 以存取說明檔或搜尋「知識庫」。如果仍找不到解決方案，則您可以向「ESET 客戶關懷」提交支援請求。我們的專家可根據此意見快速地回應您的問題，並對問題提出有效的建議。

3.2 更新設定

更新病毒資料庫及更新程式元件是提供完整防護、防止惡意代碼的一個重要部分。請特別注意其設定與作業。從主要功能表中，選取 **[更新]**，然後按一下主要程式視窗中的 **[更新病毒資料庫]**，立即檢查是否有新資料庫可用。**[使用者名稱及密碼設定...]** 會顯示一個對話方塊，請在此輸入購買時收到的「使用者名稱」及「密碼」。

如果在 ESET Smart Security 安裝期間已輸入「使用者名稱」及「密碼」，則此時不會再提示您輸入。

[進階設定] 視窗（可按 F5 存取）包含其他詳細的更新選項。**[更新伺服器:]** 下拉式功能表應設定為 **[選擇自動]**。若要設定進階更新選項，例如更新模式、Proxy 伺服器存取、存取本機伺服器上的更新及建立病毒資料庫副本 (ESET Smart Security Business Edition)，請按一下 **[設定...]** 按鈕。



3.3 受信任區域設定

「受信任區域」的設定是在網路環境中保護電腦的一個重要步驟。您可以設定要共用的「受信任區域」，允許其他使用者存取您的電腦。按一下 **[設定 > 個人防火牆 > 變更電腦在網路中的保護模式...]** 即會顯示一個視窗，可讓您設定實際網路/區域中電腦保護模式的設定。

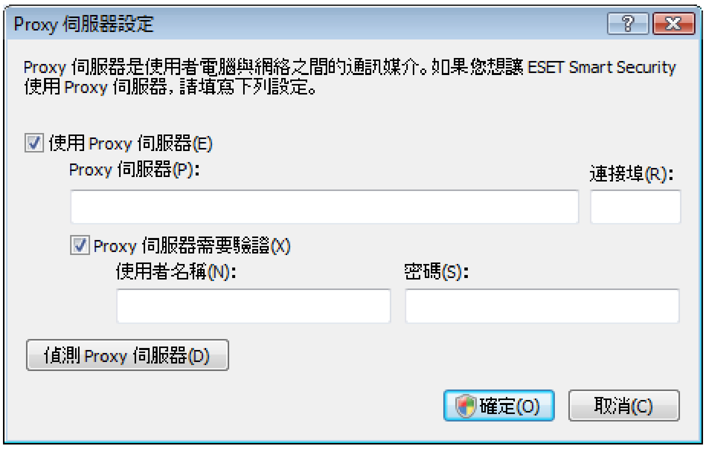
安裝 ESET Smart Security 之後或電腦連接至新網路時，會執行「受信任區域」偵測。因此，在大多數情況中無需定義「受信任區域」。依預設，偵測到新區域時會顯示對話方塊視窗，其可讓您設定該區域的保護等級。

警告！受信任區域若設定不正確，可能會對電腦造成安全風險。

附註：依預設，「受信任區域」中的工作站可存取共用檔案及印表機、啟用對內 RPC 通訊，亦可共用遠端桌面。

3.4　Proxy 伺服器設定

如果您在使用 ESET Smart Security 的系統上，利用 Proxy 伺服器調節與網際網路的連線，則必須在 [進階設定] (F5) 中進行指定。若要存取 **[Proxy 伺服器]** 設定視窗，請從 [進階設定] 樹狀目錄中按一下 **[其他選項 > Proxy 伺服器]**。選取 **[使用 Proxy 伺服器]** 核取方塊，並輸入 Proxy 伺服器的 IP 位址及連接埠，以及它的驗證資料。



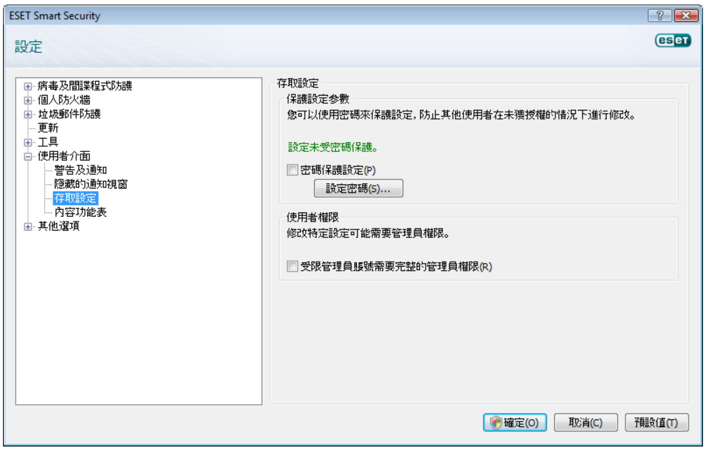
如果無法使用此資訊，則您可以嘗試透過按一下 **[偵測 Proxy 伺服器]** 按鈕，自動偵測 ESET Smart Security 的 Proxy 伺服器設定。

附註：各種更新設定檔的 Proxy 伺服器選項可能不同。如果是這種情況，請在進階更新設定中設定 Proxy 伺服器。

3.5　設定保護

「ESET Smart Security 設定」對您組織的安全原則來說非常重要。未獲授權的修改可能會危害您系統的穩定性及防護功能。若要使用密碼防護設定參數，請從主要功能表開始並按一下 **[設定 > 進入完整的進階設定樹狀目錄... > 使用者介面 > 設定保護]**，並按一下 **[輸入密碼...]** 按鈕。

輸入密碼，並重新鍵入該密碼進行確認，再按 一下 **[確定]**。未來修改任何 ESET Smart Security 設定，都需要此密碼。



4. 使用 ESET Smart Security

4.1 病毒及間諜程式防護

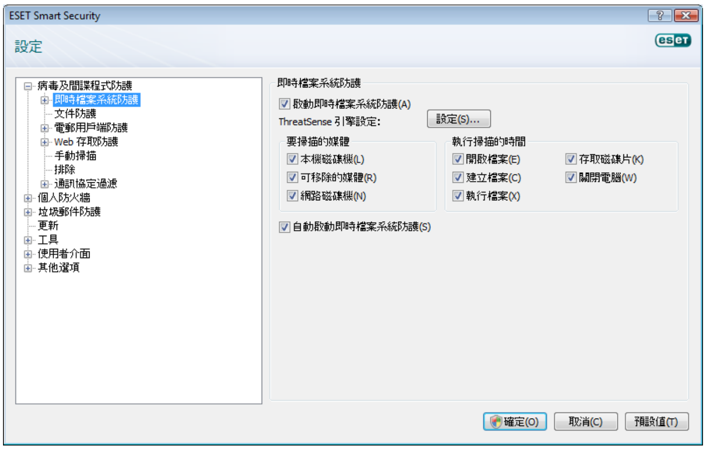
病毒防護可藉由控制檔案、電子郵件及網際網路通訊來防止惡意系統攻擊。如果偵測到含有惡意代碼的威脅，「防毒」模組會先進行封鎖，再以清除、刪除或移至隔離區等方式去除威脅。

4.1.1 即時檔案系統防護

即時檔案系統防護控制系統中與防毒相關的所有事件。開啟、建立或在電腦上執行所有檔案時，會掃描其中是否具有惡意代碼。在系統啟動時會啟動即時檔案系統防護。

4.1.1.1 控制項設定

即時檔案系統防護會檢查所有媒體類型，而且許多種事件都會觸發控制項。控制項利用 ThreatSense 技術偵測方法 (如 ThreatSense 引擎參數設定中所述)。針對新建立的檔案及現有檔案，控制行為可能有所不同。若為新建立的檔案，則可套用較深入的控制層級。



4.1.1.1.1 要掃描的媒體

依預設，會掃描所有媒體類型是否存在潛在威脅。

本機磁碟機 – 控制所有系統硬碟

可移除的媒體 – 磁碟片、USB 儲存裝置等

網路磁碟機 – 掃描所有對應的磁碟機

我們建議保留預設值，只在特殊情況下進行修改，例如掃描某些媒體而明顯減慢資料傳輸時。

4.1.1.1.2 執行掃描的時間 (事件觸發的掃描)

依預設，在開啟、執行或建立時會掃描所有檔案。我們建議您保留預設值，因為這些預設值會為電腦提供最高等級的即時防護。

[**存取磁碟片**] 選項會提供存取此磁碟時的磁碟片開機磁區控制。[**關閉電腦**] 選項提供在關閉電腦期間的硬碟開機磁區控制。雖然現在開機病毒很罕見，但是我們建議您保持啟用這些選項，因為仍有可能從其他來源受到開機病毒的感染。

4.1.1.1.3 用於新建立及已修改檔案的其他 ThreatSense 參數

新建立或新修改的檔案，受感染可能性遠高於現有的檔案。這就是程式使用其他掃描參數檢查這些檔案的原因所在。除了一般病毒資料庫的掃描方法，使用進階啟發式偵測可大幅增加偵測率。除了新建立的檔案之外，也會針對自我解壓縮檔案 (SFX) 及運行時間壓縮器 (內部壓縮的可執行檔) 進行掃描。依預設，無論檔案實際大小，最多可以掃描至巢狀壓縮檔的第 10 層。取消選取 [***預設壓縮檔掃描設定***] 選項，以修改壓縮檔掃描設定。

4.1.1.1.4 進階設定

為將即時防護時的系統蹤跡減至最小，已經掃描過的檔案將不再重複掃描 (除非檔案經過修改)。每次更新病毒資料庫之後，會立即重新掃描檔案。您可使用 [**最佳化掃描**] 選項設定此行為。如果停用此選項，所有檔案都會在每次存取時受到掃描。

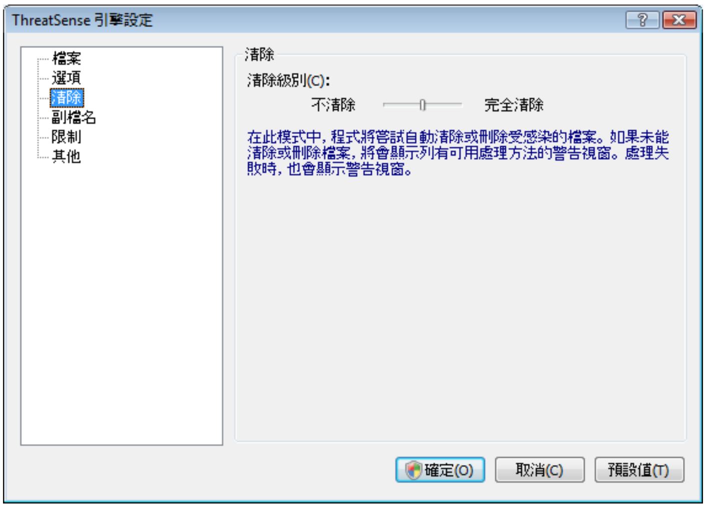
依預設，即時防護會在作業系統啟動時同時啟動，並持續提供掃描。在特殊情況下 (如與其他即時掃描器發生衝突時)，則可以停用 [**自動啟動即時檔案系統防護**] 選項，終止即時防護。

根據預設，執行檔案時不使用進階啟發式偵測。不過您可在某些情況下啟用此選項 (請勾選 [**執行檔案時的進階啟發式**] 選項)。請注意，由於進階啟發式偵測的系統需求較大，可能會降低某些程式的執行速度。

4.1.1.2 清除層級

即時防護有三種清除等級 (若要存取，請按一下 [**即時檔案系統防護**] 區段中的 [**設定...**] 按鈕，然後按一下 [**清除**] 子目錄)。

- 第一層是顯示警告視窗，針對所找到的各個入侵提供可用選項。使用者必須分別選擇各入侵的處理方法。此層級的目標使用者，是瞭解發生入侵時要採取哪些步驟的進階使用者。
- 預設層級會自動選擇並執行預先定義的處理方法 (視入侵的類型而定)。畫面右下角會顯示資訊訊息，通知受感染檔案的偵測及刪除狀況。不過，如果入侵所在的壓縮檔也包含未感染檔案，或是所在物件未預先定義處理方法，則不會執行自動的處理方法。
- 第三層最「主動」，即清除所有受感染的物件。因為此層級可能潛在導致有效檔案的遺失，所以我們建議僅在特定情況下才使用。



4.1.1.3 何時修改即時保護設定

即時防護是維護系統安全的最重要組成部分。因此，修改其參數時請小心。建議您僅在特定情況中修改其參數。例如，在與特定應用程式或另一個防毒程式的即時掃描器發生衝突的情況下。

ESET Smart Security 的所有設定在安裝後即已最佳化，為使用者提供最高等級的系統安全。若要還原預設值，請按一下位於 [**即時檔案系統防護**] 視窗 ([**進階設定 > 病毒及間諜程式防護 > 即時檔案系統防護**]) 右下方的 [**預設值**] 按鈕。

4.1.1.4 檢查即時防護

若要驗證即時防護是否運作與可否偵測到病毒，請使用來自 eicar.com 的測試檔案。此測試檔案是所有防毒程式都可偵測到的特殊無害檔案。這是 EICAR (European Institute for Computer Antivirus Research) 公司所建立的檔案，可測試防毒程式的功能。檔案 eicar.com 的下載連結為 http://www.eicar.org/download/eicar.com

附註：請先停用防火牆，再執行即時保護檢查。如果已啟用防火牆，則其會偵測到檔案並防止下載測試檔案。

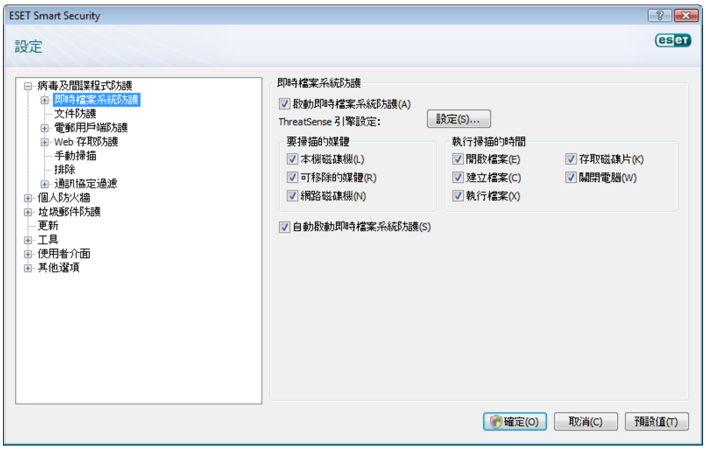
4.1.1.5 即時防護無法運作時怎麼辦

我們會在下一章說明使用即時防護時可能發生的問題情況，以及如何進行疑難排解。

已停用即時防護

如果使用者不小心停用即時防護，則必須重新啟動。若要重新啟動即時保護，請瀏覽至 [**設定 > 病毒及間諜程式防護**]，並在主要程式視窗的 [**即時檔案系統防護**] 區段中按一下 [**啟用**]。

如果系統啟動時未初始化即時防護，可能是由於已停用 [**自動啟動即時檔案系統防護**] 選項。若要啟用此選項，請瀏覽至 [**進階設定**] (F5)，並按一下 [進階設定] 樹狀目錄中的 [**即時-檔案系統防護**]。請在視窗底端的 [**進階設定**] 區段中，確認選取 [**自動啟動即時檔案系統防護**] 核取方塊。



若即時保護沒有偵測及清除入侵

請確定電腦上未安裝任何其他防毒程式。如果同時啟用兩個即時防護 Shield，則可能會互相衝突。我們建議您解除安裝系統上的任何其他防毒程式。

即時防護未啟動

若已啟用 [**自動啟動即時檔案系統防護**] 選項，但系統啟動時未初始化即時防護，則可能是由於與其他程式發生衝突。如果是這種情況，請洽詢 ESET 的「客戶關懷」專家。

4.1.2 電子郵件用戶端防護

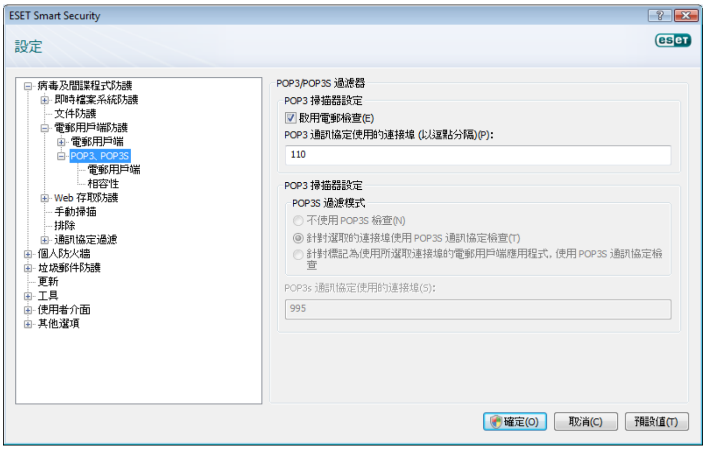
電子郵件防護可控制透過 POP3 通訊協定收到的電子郵件通訊。其使用 ESET Smart Security 這款 Microsoft Outlook 外掛程式，控制來自電子郵件用戶端的所有通訊 (POP3、MAPI、IMAP、HTTP)。檢查對內郵件時，程式會使用 ThreatSense 掃描引擎提供的所有進階掃描方法。也就是說，與病毒資料庫進行比對之前，就會進行惡意程式的偵測。POP3 通訊協定的掃描不限定所用的電子郵件用戶端。

4.1.2.1 POP3 檢查

在電子郵件用戶端應用程式中，POP3 通訊協定是接收電子郵件通訊使用最廣泛的通訊協定。無論使用的電子郵件用戶端為何，ESET Smart Security 均可保護此通訊協定。

提供此控制項的模組會自動在作業系統啟動時同時初始化，接著在記憶體中發生作用。若要讓模組正確運作，請務必啟用模組 - 系統會自動執行 POP3 檢查，無需重新設定電子郵件用戶端。依預設，通訊埠 110 中的所有通訊均會經過檢查；必要時，您也可以新增其他通訊埠。埠號必須以逗號分隔。

加密的通訊不受控制。



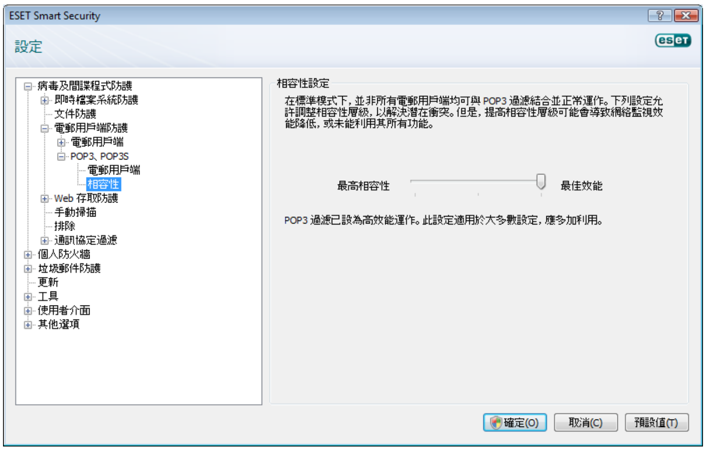
4.1.2.1.1 相容性

使用 POP3 過濾功能時，有些電子郵件程式可能會遇到問題 (例如，若接收郵件的網際網路連線較慢，則可能由於檢查而發生逾時)。如果是這種情況，請嘗試修改執行控制項的方式。降低控制等級，可能會提昇清除程序的速度。若要調整 POP3 過濾的控制等級，請瀏覽至 [**病毒及間諜程式防護 > 電子郵件防護 > POP3 > 相容性**]。

如果啟用 [**最佳效能**]，則會從受感染的郵件中移除入侵，並在原始電子郵件主旨之前插入入侵的相關資訊 (必須啟動選項 [**刪除**] 或 [**清除**]，或者必須啟用 [**完全**] 或 [**預設**] 清除等級)

[**中等相容性**] 會修改接收郵件的方式。郵件會逐步傳送至電子郵件用戶端，在傳輸郵件的最後一部分之後，再掃描郵件是否含有入侵。不過，使用此控制層級的感染風險較高。清除及處理標籤郵件 (在郵件的主旨行與內容中附加通知警告) 的等級與最佳效能設定相同。

使用 [**最高相容性**] 等級，會出現警告視窗以警告使用者，報告接收到的某郵件已受到感染。不會將任何關於受感染檔案的資訊新增至已傳遞郵件的主旨行或電子郵件內容，而且不會自動移除入侵。刪除入侵必須由使用者從電子郵件用戶端執行。

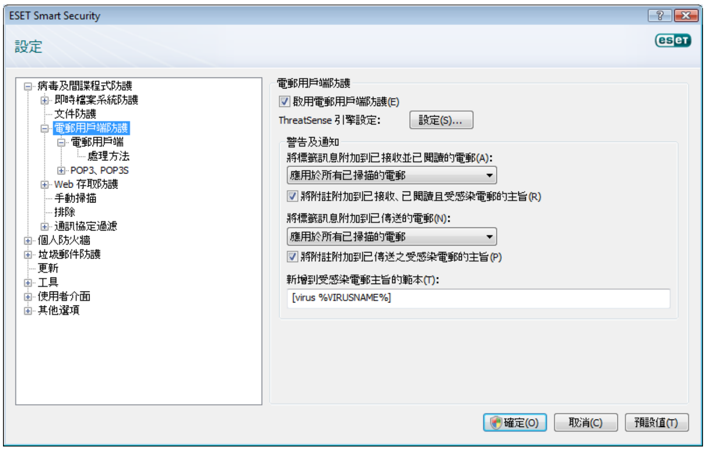


4.1.2.2 與電子郵件用戶端整合

ESET Smart Security 與電子郵件用戶端的整合會針對電子郵件中的惡意代碼，增加作用中的防護等級。如果支援電子郵件用戶端，則可以在 ESET Smart Security 中啟用此整合。如果啟動整合，則會將 ESET Smart Security Antispam 工具列直接插入電子郵件用戶端中，以更有效地進行電子郵件保護。您可以透過 [**設定 > 進入完整的進階設定樹狀目錄... > 其他選項 > 電子郵件用戶端整合**]，存取整合設定。此對話視窗可讓您啟動與受支援電子郵件用戶端的整合。目前支援的電子郵件用戶端包括 Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 及 Mozilla Thunderbird。

如果電子郵件用戶端運作時發生系統速度減慢的情形，請選取 [***停用收件匣內容變更檢查***] 選項。從 Kerio Outlook Connector Store 下載電子郵件時可能會發生此類情況。

您可啟動 [**進階設定 (F5)** > **病毒及間諜程式防護** > **電子郵件防護**] 中的 [**啟用電郵防護**] 核取方塊，啟動電子郵件防護。



4.1.2.2.1 將標籤訊息附加到電子郵件內容

ESET Smart Security 控制的每封電子郵件，都可以在主旨或電子郵件內容中附加標籤訊息，予以標記。此功能會增加收件者的可靠性等級，而且如果偵測到入侵，會提供已知電子郵件/寄件者威脅等級的相關實用資訊。

您可透過 [**進階設定 > 病毒及間諜程式防護 > 電郵用戶端防護**]，使用此功能的選項。該程式可以 [**將標籤訊息附加到已接收並已閱讀的電郵**]，且可以 [**將標籤訊息附加到已傳送的電子郵件**]。使用者還可以決定將標籤訊息附加到所有電子郵件、僅附加到受感染的電子郵件，或者完全不附加。ESET Smart Security 還允許使用者將郵件附加到受感染郵件的原始主旨。若要啟用附加到主旨，請選取選項 [**將附註附加到已接收、已閱讀且受感染電郵的主旨**] 及 [**將附註附加到已傳送之受感染電郵的主旨**]。

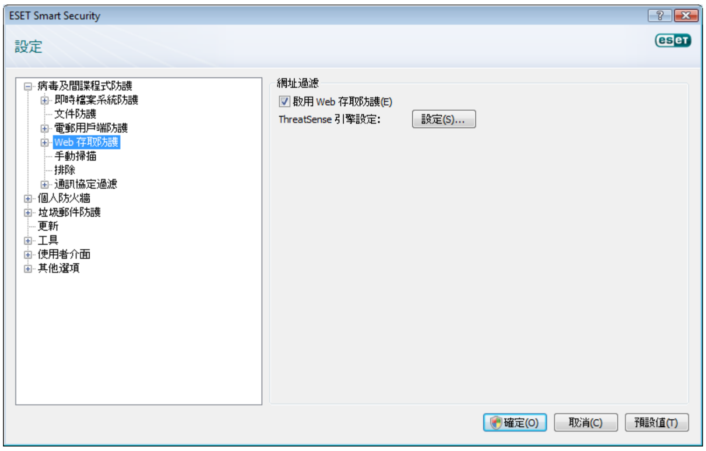
您可以在受感染電子郵件主旨新增的 [範本] 欄位中修改通知的內容。上述修改可協助您自動過濾受感染的電子郵件，因為其可讓您將具有特定主旨的電子郵件過濾到個別資料夾 (如果您電子郵件用戶端中支援的話)。

4.1.2.3 移除入侵

如果收到受感染的電子郵件訊息，會顯示警告視窗。警告視窗會顯示寄件者名稱、電子郵件，以及入侵的名稱。對於已偵測到的物件，可從在視窗下半部選用 [**清除**]、[**刪除**] 或 [**離開**] 等選項。在大多數情況下，我們建議您選取 [**清除**] 或 [**刪除**]。在特殊情況下，當您想要接收受感染的檔案時，請選取 [**離開**]。如果已啟用 [**完全清除**]，則資訊視窗上不會顯示用於受感染物件的選項。

4.1.3 Web 存取防護

網際網路連線是個人電腦中的標準功能。很遺憾，它也已成為傳輸惡意代碼的主要媒介。因此，請務必審慎考量您的 Web 存取防護措施。我們強烈建議啟動 [**啟用 Web 存取防護**] 選項。此選項位於 [**進階設定 (F5) > 病毒及間諜程式防護 > Web 存取防護**]。



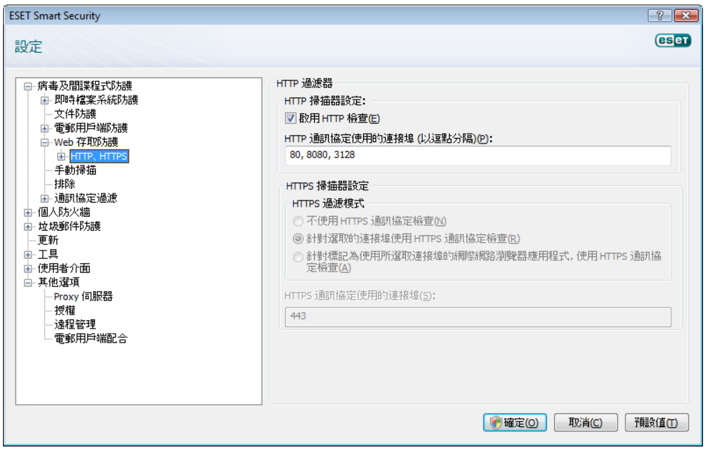
4.1.3.1 HTTP、HTTPS

Web 存取防護的運作方式是監視網際網路瀏覽器與遠端伺服器之間的通訊，並遵循 HTTP (超文字傳輸通訊協定) 及 HTTPS (加密的通訊) 規則。依預設，ESET Smart Security 已配置為使用大多數網際網路瀏覽器的標準。不過，您可以在 [Web 存取防護 > HTTP、HTTPS] 中修改 HTTP 掃描器設定選項。在主要的 [HTTP 過濾器] 視窗中，您可以選取或取消選取 [**啟用 HTTP 檢查**] 選項。您也可以定義用於 HTTP 通訊的連接埠號碼。依預設，預先定義的連接埠號為 80、8080 及 3128。HTTPS 檢查可以在下列模式中執行：

不使用 HTTPS 通訊協定檢查
不會檢查加密的通訊

針對選取的連接埠使用 HTTPS 通訊協定檢查
只針對 [HTTPS 通訊協定使用的連接埠] 中定義的連接埠進行 HTTPS 檢查

針對標記為使用所選取連接埠的網際網路瀏覽器應用程式，使用 HTTPS 通訊協定檢查
只檢查在瀏覽器區段中指定的應用程式，並使用 [***HTTPS 通訊協定使用的連接埠***] 中定義的連接埠

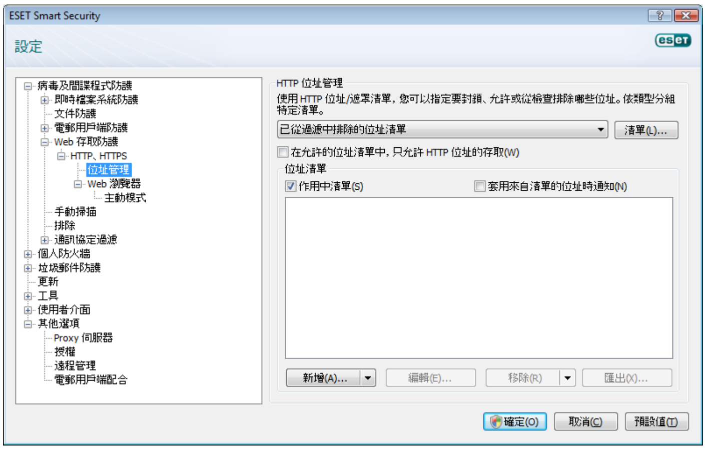


4.1.3.1.1　位址管理

本區段可讓您指定要封鎖、允許或從檢查中排除的 HTTP 位址。

按鈕 [**新增**]、[**變更**]、[**移除**] 及 [**匯出**] 可用來管理位址清單。封鎖位址清單中的網站將無法存取。已排除位址清單中的網站則可存取，而不會掃描惡意程式碼。如果您啟用 [***在允許的位址清單中，只允許 HTTP 位址的存取***]，則只能存取允許位址清單中的位址，而封鎖所有其他 HTTP 位址。

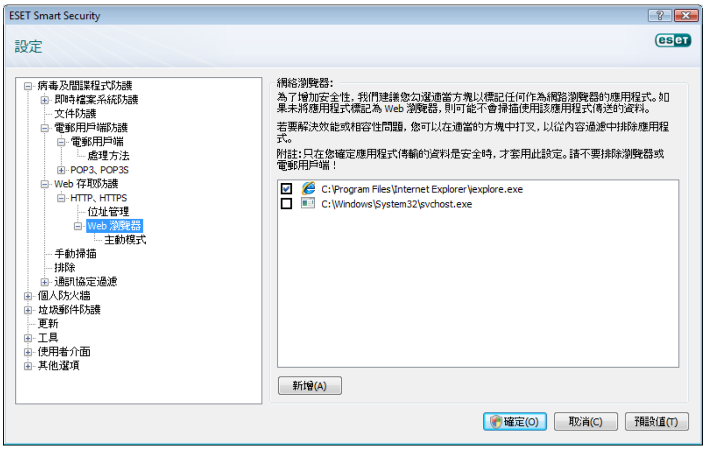
在所有清單中都可以使用特殊符號 * (星號) 及 ? (問號)。星號可替代任何字元字串，而問號可替代任何符號。指定已排除的位址時應該特別小心，因為清單應僅包含受信任及安全的位址。同樣地，必須確定在此清單中正確使用 * 及 ? 等符號。若要啟動清單，請選取 [***作用中清單***] 選項。如果您希望在進入目前清單中的位址時收到通知，請選取 [***套用來自清單的位址時通知***]。



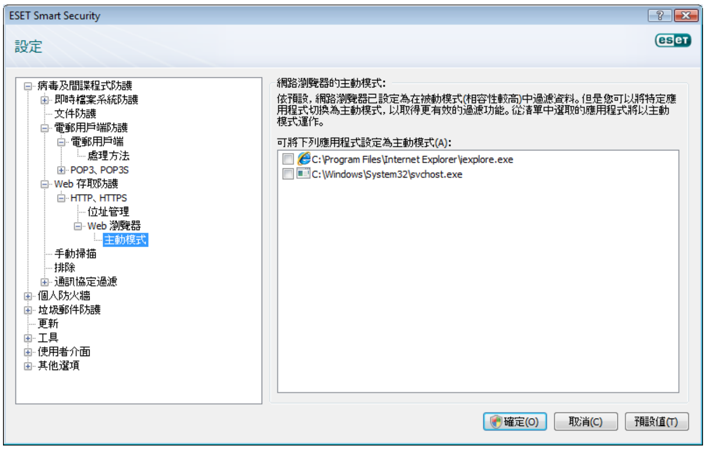
4.1.3.1.2　Web 瀏覽器

ESET Smart Security 還包含 [**Web 瀏覽器**] 功能，允許使用者定義特定應用程式是否為瀏覽器。如果使用者將某應用程式標記為瀏覽器，則無論通訊中包含的埠號為何，都會監視來自此應用程式的所有通訊。

Web 瀏覽器功能可補足 HTTP 檢查功能，因為 HTTP 檢查僅作用於預先定義的連接埠。不過，許多網際網路服務利用動態變更或不明的埠號。為達到此目的，Web 瀏覽器功能可控制通訊埠通訊，無論連線參數為何。



您可直接從 [**HTTP**] 子目錄的 [**Web 瀏覽器**] 子功能表，存取標記為瀏覽器的應用程式清單。此區段還包含定義網際網路瀏覽器之檢查模式的子功能表 [**主動模式**]。[**主動模式**] 非常實用，因為它會整體檢查傳輸的資料。如果未啟用此功能，則會以批次方式逐步監視應用程式的通訊。此模式會降低資料驗證程序的效率，但是也會針對列出的應用程式提供更高的相容性。如果在使用期間未發生任何問題，則我們建議您選取所需應用程式旁邊的核取方塊，啟用主動檢查模式。



4.1.4　電腦掃描

如果您懷疑電腦受感染 (行為異常)，請執行手動電腦掃描以檢查電腦是否含有入侵。從安全觀點來看，不僅應於懷疑有感染時執行電腦掃描，也應將此視為例行安全考量的一部分，定期執行掃描。有些入侵未被即時掃描器偵測出，就儲存至磁碟，而定期掃描可偵測到這些入侵。若在停用即時掃描器期間受到感染，或病毒資料庫已過時，就可能發生上述情況。

我們建議您一個月至少執行一至兩次指定掃描。您可以透過 [**工具** > [**排程器**] 將掃描設定為排定的工作。

4.1.4.1　掃描類型

有兩種可用的類型。[**標準掃描**]　可快速掃描系統，而無需進一步設定掃描參數。[**自訂掃描...**] 允許使用者選取任何預先定義的掃描設定檔，以及從樹狀結構中選擇掃描物件。

4.1.4.1.1　標準掃描

標準掃描是一種簡單易用的方法，允許使用者快速啟動電腦掃描並清除受感染的檔案，而無需使用者介入。它的主要優點是可以輕鬆執行作業，而不需要詳細的掃描配置。標準掃描會檢查本機磁碟機上的所有檔案，且會自動清除或刪除偵測到的入侵。清除層級會自動設為預設值。如需清除類型的詳細資訊，請參閱「清除」(請參閱第 18 頁)。

標準掃描設定檔的目標使用者，是希望快速輕鬆掃描電腦的使用者。此設定檔提供有效的掃描及清除解決方案，而無須繁複的配置過程。

4.1.4.1.2 自訂掃描

如果您希望指定掃描參數 (例如掃描目標及掃描方法)，則可選用自訂掃描這個解決方案。「自訂」掃描的優點是可以詳細地設定參數。您可以將設定儲存至使用者定義的掃描設定檔，以利於使用相同參數重複執行掃描。

若要選取掃描目標，請使用快速目標選擇功能的下拉式功能表，或從列出電腦上所有可用裝置的樹狀結構中選取目標。您亦可進一步使用下列方法選用三種清除等級：按一下 [**設定... > 清除**]。如果您僅有意掃描系統而不想執行其他處理方法，請選取 [**掃描但不清除**] 核取方塊。

對於具有先前使用防毒程式經驗的使用者，使用 [自訂] 掃描模式執行電腦掃描比較適合。

4.1.4.2 掃描目標

[掃描目標] 下拉式功能表可讓您選取要進行病毒掃描的檔案、資料夾及裝置 (磁碟)。

您可使用快速掃描目標功能表選項，選取下列目標：

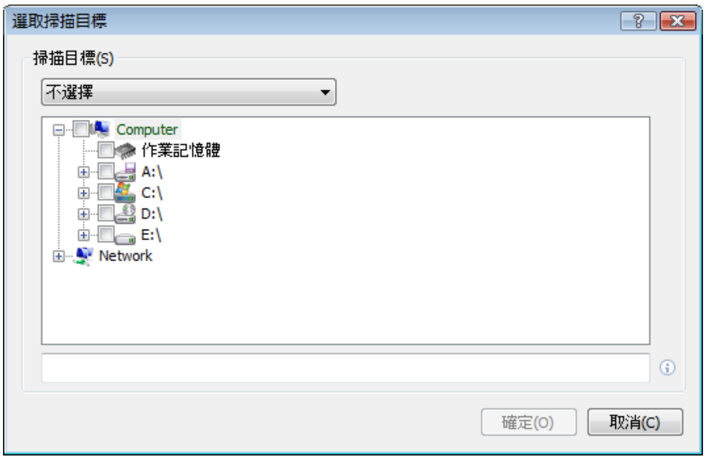
使用設定檔設定 – 控制所選掃描設定檔設定的目標

可移除的媒體 – 磁碟片、USB 儲存裝置、CD/DVD

本機磁碟機 – 控制所有系統硬碟

網路磁碟機 – 所有對應的磁碟機

不選擇 – 取消所有選擇



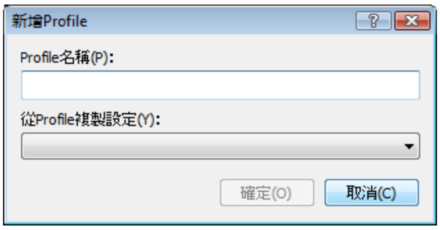
亦可輸入您希望納入掃描的資料夾或檔案路徑，更精確地指定掃描目標。從列出電腦上所有可用裝置的樹狀結構中選取目標。

4.1.4.3 掃描設定檔

您可將偏好的電腦掃描參數儲存為設定檔。建立掃描設定檔的優點是，可用於日後的定期掃描。我們建議您依使用者日常使用的需求，建立含有不同掃描目標、掃描方法及其他參數等多個設定檔。

若要建立可重複用於未來掃描的新設定檔，請瀏覽至 [**進階設定 (F5) > 手動電腦掃描**]。按一下右邊的 [**設定檔...**] 按鈕，以顯示現有掃描設定檔的清單，以及建立新設定檔的選項。下列 **ThreatSense 引擎參數設定**說明掃描設定中的各參數。這樣可協助您依個人需求建立掃描設定檔。

範例：
假設指定至 [**智慧型掃描**] 設定檔的設定不盡符合您的需求，而希望自行建立掃描設定檔。但是，您不希望掃描運行時間壓縮器或潛在危險的應用程式，且希望套用 [**完全清除**]。請從 [**修改Profile**] 視窗中，按一下 [**新增...**] 按鈕。在 [**設定檔名稱**] 欄位中，輸入新設定檔的名稱，並從 [**從設定檔複製設定:**] 下拉式功能表中選取 [**智慧型掃描**]。然後調整其他的參數，以符合您的需求。



4.1.5 通訊協定篩選

應用程式通訊協定 POP3 及 HTTP 的病毒防護由 ThreatSense 掃描引擎提供，該引擎可密切地整合所有進階惡意軟體掃描技術。無論是使用網際網路瀏覽器還是電子郵件用戶端，都會自動執行控制。通訊協定過濾可以使用下列選項 (如果開啟 [**啟用應用程式通訊協定過濾**] 選項的話)：

HTTP 及 POP3 連接埠 – 限定掃描已知 HTTP 及 POP3 連接埠的通訊。

已標記為網路瀏覽器與電郵用戶端的應用程式 - 啟用此選項，則只會對標記為瀏覽器 ([Web 存取防護 > HTTP、HTTPS > Web 瀏覽器]) 及電子郵件用戶端 ([電子郵件用戶端防護 > POP3、POP3S > 電子郵件用戶端]) 的應用程式過濾通訊。

連接埠及標記為網際網路瀏覽器或電子郵件用戶端的應用程式 - 同時檢查連接埠及瀏覽器是否包含惡意軟體

附註：
從 Windows Vista Service Pack 1 與 Windows Server 2008 起，使用新的通訊過濾方式。因此，無法使用 [通訊協定過濾] 區段。

4.1.5.1 SSL

ESET Smart Security 4 可讓您檢查以 SSL 通訊協定封裝的通訊協定。您可以根據使用信任憑證、未知憑證或從 SSL 防護通訊檢查中排除之憑證的 SSL 防護通訊，使用不同掃描模式。

一律掃描 SSL 通訊協定 (已排除及受信任的憑證持續有效) – 若選取此選項，則除了排除不予檢查的憑證所防護的通訊之外，SSL 防護的所有通訊都會受到掃描。若有新通訊採用未知、已簽署的憑證，則會自動過濾此通訊，使用者不會收到任何告知。若使用者存取的伺服器中含有不信任憑證，但該憑證已由使用者標示為可信任 (將其新增至信任憑證清單)，則會允許與此伺服器的通訊，而過濾通訊通道的內容。

詢問未造訪的網站 (未知憑證) – 如果您輸入新的 SLL 防護網站 (具有未知憑證)，則會顯示處理方法選擇對話方塊。此模式可讓您建立要排除不予掃描的 SSL 憑證清單。

不掃描 SSL 通訊協定 - 如果選取此選項，則程式將不會掃描透過 SSL 進行的通訊。

如果憑證無法通過「受信任的系統管理員憑證機關中心」驗證

詢問憑證有效性 – 提示使用者選取要採取的處理方法

封鎖使用憑證的通訊 – 終止與使用該憑證之網站的連線

如果憑證無效或損毀

詢問憑證有效性 – 提示使用者選取要採取的處理方法

封鎖使用憑證的通訊 – 終止與使用該憑證之網站的連線

4.1.5.1.1 可信任的憑證

除了 ESET Smart Security 4 儲存信任憑證的整合「受信任的系統管理員憑證機關中心」外，您也可以建立信任憑證的自訂清單，可在 [**設定 (F5)** > **通訊協定過濾** > **SSL** > **可信任的憑證**] 中檢視。

4.1.5.1.2 排除的憑證

[排除的憑證] 區段中包含被視為安全的憑證。以清單中憑證加密的通訊內容，不會受到檢查。我們建議您僅安裝有安全保證而無需執行內容過濾的網站憑證。

4.1.6 ThreatSense 引擎參數設定

ThreatSense 這種技術，是由複雜威脅偵測方法所組成的。此技術是主動式的，也就是說它也可在新威脅擴散的最初幾小時間提供保護。其使用多種方法組合 （代碼分析、代碼模擬、一般資料庫、病毒資料庫)，共同合作以大幅增強系統安全性。掃描引擎可以同時控制數個資料串流，以最大化效能及偵測率。ThreatSense 技術還可以順利消除 rootkit。

ThreatSense 技術設定選項可讓使用者指定數種掃描參數：

- 要掃描的檔案類型及副檔名
- 各種偵測方法的組合
- 清除的等級等

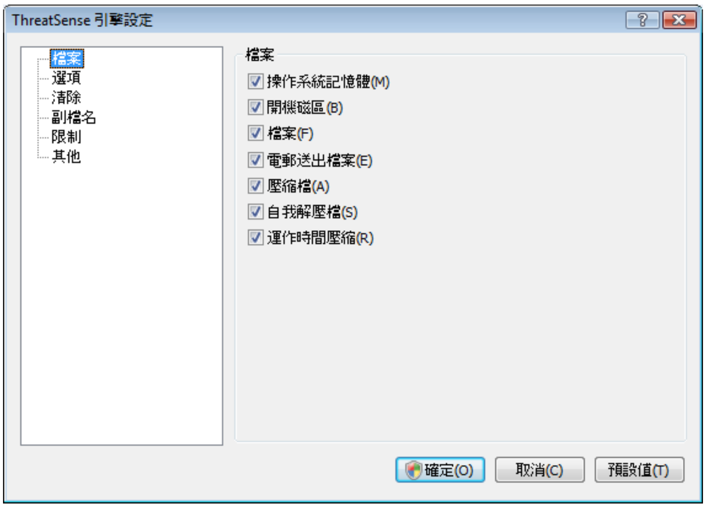
若要進入設定視窗，請在使用 ThreatSense 技術的任何模組設定視窗中，按一下 [**設定...**] 按鈕 (如下所示)。不同的安全情況可能需要不同的設定。瞭解這一點之後，就可針對下列防護模組，分別進行 ThreatSense 設定：

- 即時檔案系統防護
- 系統啟動檔案檢查
- 電子郵件防護
- Web 存取防護
- 手動電腦掃描

每個模組的 ThreatSense 參數都已高度最佳化，修改的話可能會對系統作業造成大幅影響。例如，將參數變更為一律掃描運行時間壓縮器，或在即時檔案系統防護模組中啟用進階啟發式偵測，可能會導致系統速度減慢 (這些方法通常僅用來掃描新建立的檔案)。因此，除了 [電腦掃描] 之外，我們建議您不要變更任何模組的預設 ThreatSense 參數。

4.1.6.1 物件設定

[**物件**] 區段可讓您定義要掃描入侵的電腦元件和檔案。



作業記憶體 – 掃描攻擊系統作業記憶體的威脅。

開機磁區 – 掃描開機磁區的主要開機記錄中是否存在病毒

檔案 – 掃描所有一般檔案類型(程式、圖片、音訊檔、視訊檔、資料庫檔案等)

電子郵件檔案 – 掃描包含電子郵件的特殊檔案

壓縮檔 – 掃描壓縮檔 (.rar、.zip、.arj、.tar 等) 中壓縮的檔案

自我解壓檔 - 掃描自我解壓檔中包含的檔案，通常副檔名為 .exe

運行時間壓縮器 – 除了 UPX、yoda、ASPack、FGS 等標準靜態壓縮器之外，運行時間壓縮器 (不同於標準壓縮檔類型) 會在記憶體中解壓縮。

4.1.6.2 選項

使用者可以在 [選項] 區段中，選取在掃描系統是否遭到入侵時要使用的方法。可用選項如下：

簽章 – 簽章可以準確可靠地依使用病毒資料庫的入侵名稱，偵測及識別入侵。

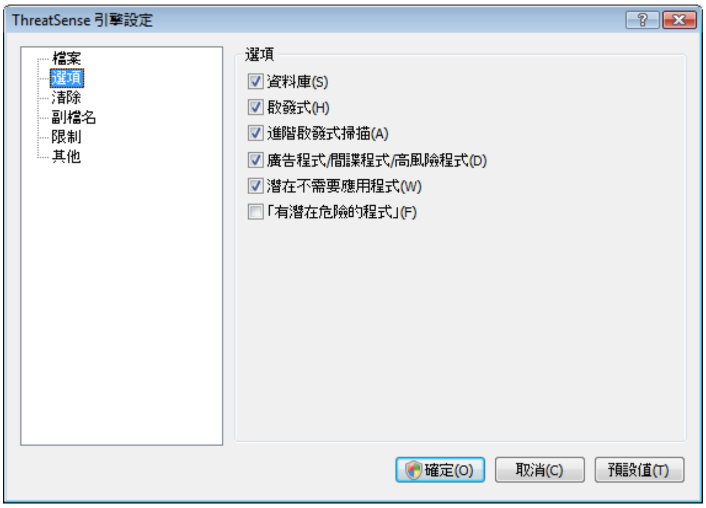
啟發式偵測 – 啟發式偵測是分析程式 (惡意) 活動的演算法。啟發式偵測的主要優點是可以偵測之前不存在或不在已知病毒清單 (病毒資料庫) 中的新惡意軟體。

進階啟發式偵測 – 進階啟發式包含 ESET 開發的獨特啟發式偵測演算法，針對電腦蠕蟲及特洛伊木馬程式的偵測功能進行最佳化之後，以高階程式設計語言撰寫而成。進階啟發式偵測大幅提昇了程式的偵測智能。

廣告程式/間諜程式/高風險程式 – 此類別包括未經使用者同意即收集各種敏感資訊的軟體。此類別也包括顯示廣告資料的軟體。

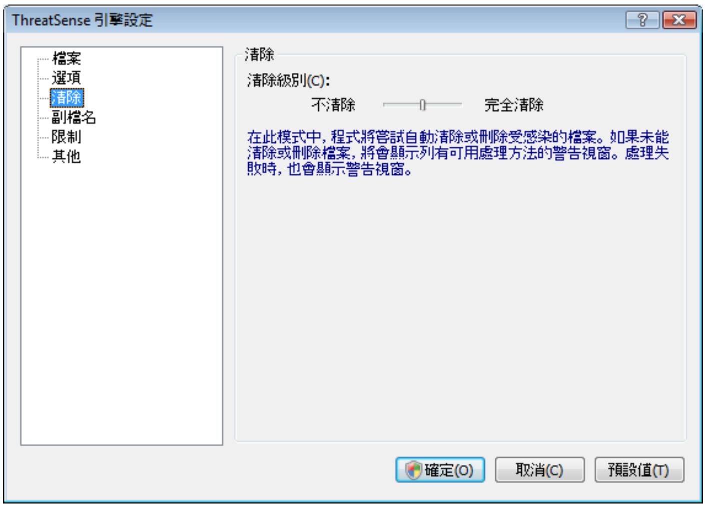
有潛在危險的程式 – 有潛在危險的應用程式是用於合法商業軟體的類別。此類別包括如遠端存取工具等程式，因此預設停用此選項。

潛在不需要應用程式 – 潛在不需要應用程式不一定是惡意的，但是對電腦效能可能會造成負面影響。這些應用程式通常需要經過同意才能安裝。如果您的電腦上有這類應用程式，系統的表現會與安裝這類應用程式之前有所不同。最明顯的變更像是：出現不需要的快顯視窗、啟動及執行隱藏程序、系統資源的用量增加、搜尋結果有所不同，以及應用程式會與遠端伺服器進行通訊。



4.1.6.3 清除

清除設定會決定掃描器清除受感染檔案期間的行為。有 3 個清除等級：



不清除
不會自動清除受感染的檔案。程式會顯示警告視窗並允許使用者選擇處理方法。

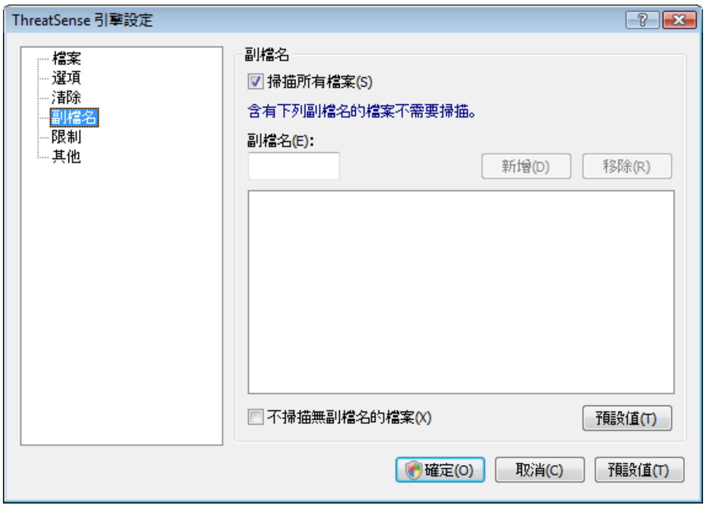
預設層級
程式會嘗試自動清除或刪除受感染檔案。如果無法自動選取正確的處理方法，則程式會提供後續處理方法的選項。無法完成預先定義的處理方法時，也會顯示後續處理方法的選項。

完全清除
程式會清除或刪除所有受感染檔案 (包括保存檔)。只有系統檔案例外。如果無法清除檔案，則會在警告視窗中為使用者提供可採取的處理方法。

警告：
在［預設］模式中，只有在壓縮檔中的所有檔案都受到感染時，才會刪除整個壓縮檔。如果壓縮檔中包含合格檔案，則不會進行刪除。如果在［完全清除］模式中偵測到受感染的壓縮檔，即使有其中有未感染的檔案，亦會刪除整個壓縮檔。

4.1.6.4 副檔名

副檔名是檔案名稱中以句點隔開的部份。副檔名定義檔案的類型及內容。ThreatSense 參數設定的此區段可讓您定義要掃描的檔案類型。



依預設，會掃描所有檔案，無論其副檔名為何。您可以將任何副檔名新增至排除不予掃描的檔案清單。如果取消勾選［**掃描所有檔案**］選項，則清單會變更為顯示目前掃描的所有檔案副檔名。您可以使用［**新增**］及［**移除**］按鈕，啟用或禁止掃描某些副檔名。

若要啟用掃描無副檔名的檔案，請選取 [**掃描無副檔名的檔案**] 選項。

若掃描某些檔案類型會造成使用這些副檔名的程式無法正常執行，就必須排除這種檔案類型不予掃描。例如，使用 MS Exchange 伺服器時，可排除 .edb、.eml 及 .tmp 等副檔名。

4.1.6.5 限制

[限制] 區段可讓您指定要掃描的物件大小上限，以及巢狀壓縮檔層級：

物件大小上限 (位元組)
定義要掃描的物件大小上限。之後特定防毒模組就只會掃描小於所指定大小的物件。我們不建議變更預設值，因為通常無需修改。只有進階使用者基於特定的理由，才應變更此選項以排除掃描較大物件。

物件掃描時間上限 (秒)
定義掃描物件的時間值上限。如果在這裡輸入使用者定義的值，則當該時間到期，無論掃描是否完成，防毒模組都會停止掃描物件。

檔案層度等級
指定壓縮檔掃描的深度上限。不建議變更預設值 10；在正常情況下，應該沒有必要修改。如果由於巢狀壓縮檔的數目而提前結束掃描，則壓縮檔會保持未檢查狀態。

壓縮檔中檔案的大小上限 (位元組)
此選項可讓您指定要掃描的壓縮檔中，所包含檔案 (解壓縮後) 的大小上限。如果由於該原因而提前結束壓縮檔的掃描，則壓縮檔會保持未檢查狀態。

4.1.6.6 其他

掃描替代資料串流 (ADS)
NTFS 檔案系統使用的替代資料串流 (ADS)，其中的檔案及資料夾關聯無法使用一般掃描技術無法看到。許多入侵會透過將自己偽裝為替代資料串流，試圖躲避偵測。

以低優先順序執行背景掃描
每個掃描序列都會消耗大量的系統資源。若您操作的程式佔用大量的系統資源，則可以啟動低優先順序背景掃描，以節省資源供您的應用程式使用。

記錄所有物件
如果已選取此選項，則防護記錄檔案會顯示所有已掃描的檔案 (包括未受感染的檔案)。

保存最後一次的存取時間郵戳
勾選此選項，以保留掃描檔案的原始存取時間，而不會更新該時間 (例如，可用於資料備份系統)。

捲動防護記錄
此選項可讓您啟用/停用防護記錄捲動。如果選取此選項，資訊會在顯示視窗中向上捲動。

在個別視窗中顯示掃描完成通知
會開啟獨立視窗，其中包含個別掃描結果資訊。

4.1.7 偵測到入侵

入侵會從不同的進入點、網頁、共用資料夾、電子郵件，或從抽取式電腦裝置 (USB、外部磁碟、CD、DVD、磁碟片等) 到達系統。

如果您的電腦出現速度變慢、經常停止等惡意軟體感染的徵兆，建議您執行下列各項作業：

- 開啟 ESET Smart Security，並按一下 [**電腦掃描**]
- 按一下 [**標準掃描**] (如需相關資訊，請參閱「標準掃描」)。
- 完成掃描之後，請檢閱已掃描、受感染及已清除的檔案防護記錄。

如果您僅想要掃描磁碟的某一部分，請按一下 [**自訂掃描**]，並選取要進行病毒掃描的目標。

我們舉個一般範例說明 ESET Smart Security 如何處理入侵，假設使用 [預設] 清除等級的即時檔案系統監視器偵測到入侵。則會嘗試清除或刪除檔案。若即時防護模組中未預先定義處理方法，則會要求您在警告視窗中選取一個選項。通常，可以使用 **[清除]**、**[刪除]** 及 **[離開]** 選項。不建議選取 **[離開]**，因為此選項會以原貌保留受感染的檔案。但若您確定檔案無害，只是因失誤而偵測為入侵，則可破例選用此選項。

清除及刪除
如果已將惡意代碼連接至已清除檔案的病毒已攻擊清除檔案，則套用清除。在這種情況下，會先嘗試清除受感染的檔案，將其還原到原始狀態。如果該檔案僅由惡意代碼組成，則會進行刪除。

如果受感染的檔案「已鎖定」或正由系統程序使用，則通常只會在釋放之後才能刪除 (通常在系統重新啟動後)。

刪除壓縮檔中的檔案
在［預設］清除模式中，只有在整個壓縮檔中的所有檔案都受到感染，無未受感染的檔案時，才會進行刪除。也就是說，如果壓縮檔還包含無害的未感染檔案，則不會進行刪除。但執行「完全」清除掃描時請小心，因為在「完全」清除模式中，只要壓縮檔內含有至少一個受感染的檔案時，即無論壓縮檔中其他檔案的狀態為何，都會刪除壓縮檔。

4.2 個人防火牆

[個人防火牆]　可控制所有由系統接收及發出的網路流量。此作業係以指定過濾規則為根據，藉此達成允許或拒絕個別網路連線。它可提供保護以免於遭受遠端電腦的攻擊，並封鎖某些服務。另可提供 HTTP 及 POP3 通訊協定的防毒保護。此功能是電腦安全中非常重要的一個元素。

4.2.1 過濾模式

ESET Smart Security [個人防火牆] 有三個篩選模式可用。防火牆行為會根據所選模式而不同。過濾模式也會影響需要使用者互動的層級。

您可以使用五種模式之一執行過濾：

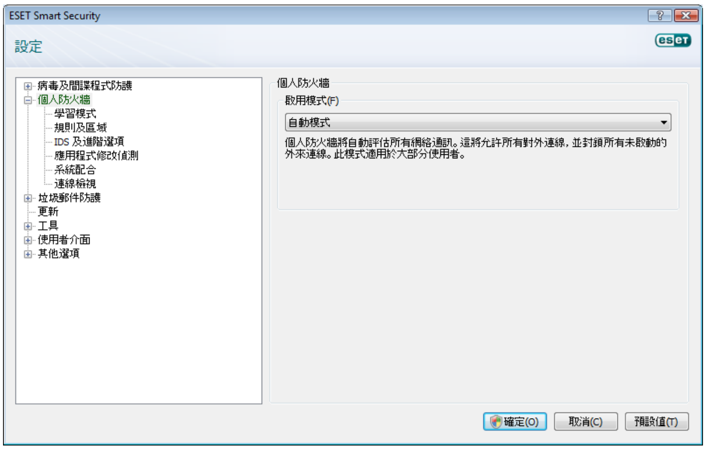
- 自動過濾模式是預設模式。適用於喜歡簡便易行的防火牆使用方法而無需定義規則的使用者。自動模式允許特定系統的所有對外流量，並封鎖網路端所起始的所有新連線。

- 發生例外情況的自動模式 (使用者定義的規則)。除了自動模式之外，還可讓您新增自訂規則。

- 互動過濾模式可讓您量身訂做適用的「個人防火牆」配置。當偵測到通訊但沒有適用於該通訊的規則時，會顯示一個對話方塊視窗，報告不明連線。該對話方塊視窗提供允許及拒絕通訊的選項，且會將允許或拒絕的決定記錄為個人防火牆的新規則。如果此時使用者選擇建立新規則，則會根據該規則，允許或封鎖將來所有此類型的連線。

- 規則模式會封鎖允許連線之特定規則所沒有定義的所有連線。此模式允許進階使用者定義僅允許所需及安全連線的規則。[個人防火牆] 會封鎖所有其他未指定的連線。

- 學習模式會自動建立及儲存規則，適用於［個人防火牆］的起始設定。此模式不需要使用者互動，因為 ESET Smart Security 會根據預先定義的參數儲存規則。[學習] 模式並不安全，請僅於已針對必要的通訊建立所有規則時才使用。



4.2.2 封鎖所有流量：中斷網路

完全封鎖所有網路流量的唯一選項是使用 **[封鎖所有網路流量：中斷網路]** 選項。[個人防火牆] 會封鎖任何對外或外來通訊，不顯示任何警告。請僅當您懷疑有嚴重安全風險，需要中斷系統與網路連線時，才使用此封鎖選項。

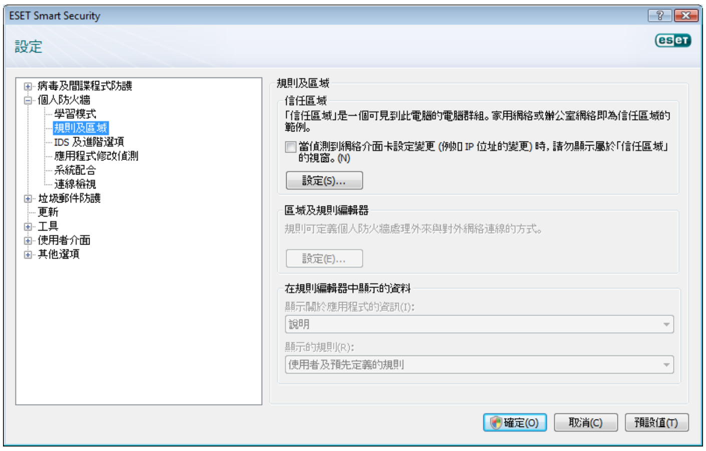
4.2.3 停用過濾：允許所有連線

[停用過濾] 選項是上述封鎖所有通訊的相反設定。如果選取，則會關閉所有 [個人防火牆] 過濾選項，允許所有對內及對外連線。在網路方面，相當於沒有防火牆存在。

4.2.4 配置及使用規則

規則代表一組條件，其可用來依目的測試所有網路連線及所有指派給這些條件的處理方法。在［個人防火牆］中，如果已建立由規則定義的連線，則您可以定義要採取的處理方法。

若要存取規則過濾設定，請瀏覽至 [**進階設定**] (F5) > [**個人防火牆**] > [**規則及區域**]。若要顯示目前設定，請按一下［**區域及規則編輯器**］區段中的［**設定...**］(如果「個人防火牆」設定為 [**自動過濾模式**]，則無法使用這些設定)。



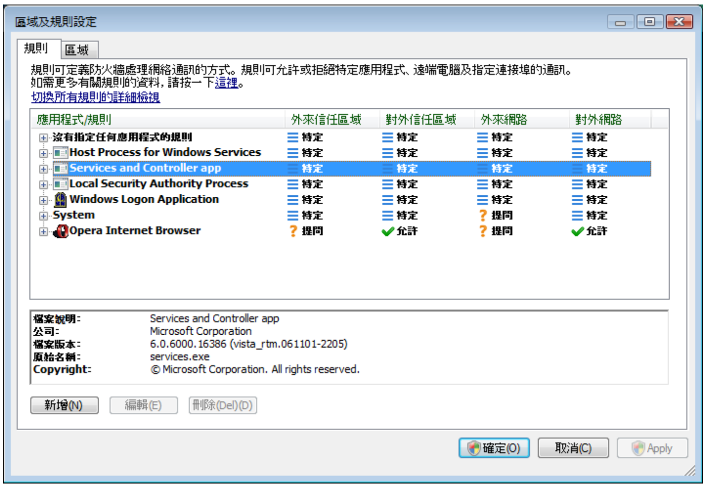
在［**區域及規則設定**］視窗中，會根據目前選取的索引標籤顯示規則或區域的概觀。視窗劃分為兩個區段。上半部列出縮短之視圖中的所有規則。下半部顯示上半部中目前已選取的規則詳細資料。在最底部為 [**新增**]、[**編輯**] 及 [**刪除**]，可讓使用者設定規則。

以通訊方向而言，可將連線劃分為對內及對外連線。對內連線由遠端電腦啟動，嘗試建立與本機系統的連線。對外連線則相反，由本機聯絡遠端電腦。

如果偵測到新的不明通訊，則您必須仔細考量要允許或拒絕。來路不明、不安全或完全不明的連線會對系統造成安全風險。如果建立此類連線，則建議您特別注意嘗試連接您電腦的遠端及應用程式。許多入侵會嘗試取得及傳送私人資料，或將其他惡意應用程式下載到主機工作站。[個人放火牆] 允許使用者偵測及終止此類連線。

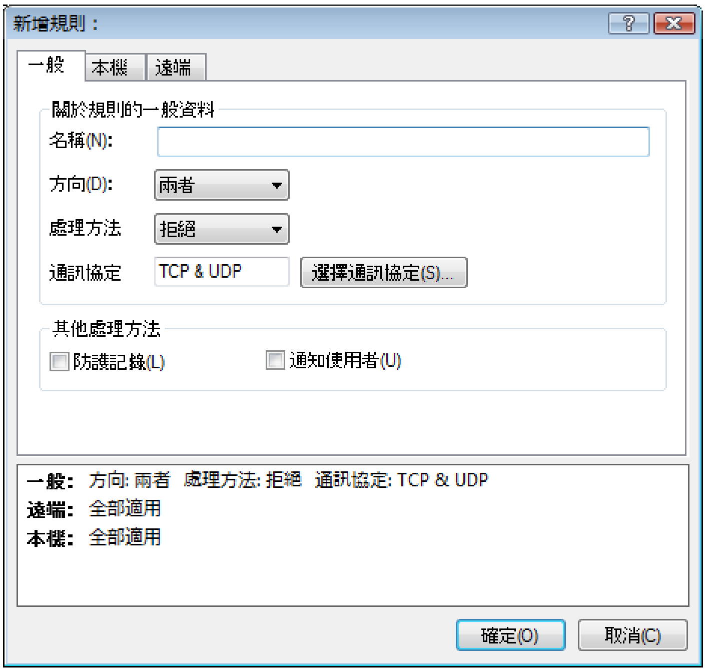
4.2.4.1 建立新規則

當安裝存取網路的新應用程式，或修改現有連線 (遠端、連接埠號碼等) 時，必須建立新的規則。



若要新增規則，請確認已選取 [**規則**] 索引標籤。然後，按一下 [**區域及規則**] 設定視窗中的［**新增**］按鈕。按一下此按鈕即，會開啟允許指定新規則的新對話視窗。視窗的上部分包含三個索引標籤：

- 一般：指定規則名稱、方向、處理方法，以及通訊協定。方向為對內或對外 (或兩者)。處理方法表示允許或拒絕特定連線。
- 本機：顯示本機連線的相關資訊，包括本機連接埠的號碼或連接埠範圍，以及通訊應用程式的名稱。
- 遠端：此索引標籤包含遠端連接埠 (連接埠範圍) 的相關資訊。亦可讓使用者定義特定規則遠端 IP 位址或區域的清單。



新增規則的良好範例為允許網際網路瀏覽器存取網路。在此情況中必須提供下列內容：

- 在 [**一般**] 索引標籤上，啟用透過 TCP 及 UDP 通訊協定對外通訊
- 將代表瀏覽器應用程式 (以 Internet Explorer 而言，為 iexplore.exe) 的處理程序新增到 [**本機**] 索引標籤上
- 在 [**遠端**] 索引標籤上，如果要僅允許標準「全球資訊網」服務，請啟用連接埠號碼 80

4.2.4.2 編輯規則

若要修改現有規則，請按一下 [**編輯**] 按鈕。上述所有參數均可加以修改 (如「建立新規則」一章所述)。

只要監視的參數有所變更，就需要修改。因此，規則不滿足條件，且無法套用指定處理方法。最後，特定連線可能遭到拒絕，導致此應用程式作業出現問題。遠端網路位址或連接埠號碼的變更就是一個範例。

4.2.5 配置區域

區域表示建立一個邏輯群組的網路位址集合。特定群組中的每個位址，都會被指派整個群組集中定義的類似規則。此類群組的一個範例為「信任區域」。「信任區域」表示完全受使用者信任，且決不會被［個人防火牆］封鎖的一組網路位址。

您可以使用 [**區域及規則設定**] 視窗中的 [**區域**] 索引標籤，按一下 [**新增**] 按鈕來設定這些區域。將區域名稱、其說明及網路位址清單輸入到新開啟的視窗中。

4.2.6　　建立連線 - 偵測

[個人防火牆] 會偵測到每個新建立的網路連線。作用中的防火牆模式 ([自動]、[互動]、[規則]) 可決定要針對新規則執行的處理方法。啟動 [自動] 或 [規則] 模式時，[個人防火牆] 會執行預先定義的處理方法，而無需使用者介入。互動模式會顯示資訊視窗，報告偵測到新網路連線，並附有連線的詳細資訊。使用者可以選擇允許或拒絕（封鎖）連線。如果您在對話方塊視窗中重複允許同一連線，則建議您針對該連線建立新的規則。若要達成此目的，請選取 [**記憶處理方法**] 選項 (建立原則)，並將處理方法儲存為 [個人防火牆] 的新規則。之後若防火牆識別到相同連線，就會套用現有規則。

建立新規則時請小心，且僅允許安全的連線。如果允許所有連線，那麼 [個人防火牆] 就失去用途了。重要的連線參數如下所示：

- **遠端**：僅允許連線到受信任的已知位址
- **本機應用程式**：不建議允許不明應用程式及處理程序的連線
- **連接埠號碼**。一般連接埠上的通訊（如 Web 連接埠號碼 80）通常是安全的

為求擴散，電腦入侵通常會使用網際網路及隱藏的連線來協助它們感染遠端系統。如果正確地設定規則，則 [個人防火牆] 會成為抵禦各種惡意代碼攻擊的實用工具。

4.2.7　　記錄

ESET Smart Security 的 [個人防火牆] 會將所有重大事件儲存在防護記錄檔案中，您可以從主要功能表直接檢視該檔案。按一下 [**工具 > 防護記錄檔案**]，然後從 [**防護記錄**] 下拉式功能表中選取 [**ESET 個人防火牆防護記錄**]。

對於偵測錯誤及揭露系統入侵來說，防護記錄檔案是珍貴的工具，且應給予適當的重視。「ESET 個人防火牆防護記錄」包含下列資料：

- 事件的日期及時間
- 事件的名稱
- 來源及目標網路位址
- 網路通訊協定
- 套用的規則或蠕蟲名稱 (如果識別)
- 涉及的應用程式

全面分析此此資料，有助於偵測到嘗試影響系統安全的行為。許多其他因素指出潛在的安全風險，並可讓使用者將其影響降至最小：經常與不明位置連線、多次嘗試建立連線、不明應用程式通訊或不常使用的連接埠號碼。

4.3　垃圾郵件防護

現在，來路不明的電子郵件（垃圾郵件）已成為電子通訊的最大問題。其數量佔了所有電子郵件通訊的 80 %。垃圾郵件防護可用來針對此問題進行保護。垃圾郵件防護模組結合數種非常有效的原則，提供卓越的過濾成效。

垃圾郵件偵測中的一個重要原則是：可以根據預先定義的信任（白名單）及垃圾郵件位址 (黑名單)，識別來路不明的電子郵件。電子郵件用戶端的所有位址及使用者標記為安全的所有其他位址，都會自動新增至 [白名單]。

偵測垃圾郵件的主要方法，是掃描電子郵件屬性。根據基本「垃圾郵件防護」條件（郵件定義、統計啟發式、識別演算法及其他單一方法）掃描收到的郵件，產生的索引值可判斷郵件是否為垃圾郵件。

在過濾中也會利用貝氏過濾。使用者可將郵件標記為***垃圾郵件***及***非垃圾郵件***，建立出要用於各自類別中的文字資料庫。資料庫越大，其產生的結果就越準確。

上述方法的組合會提供高「垃圾郵件防護」偵測率。

ESET Smart Security 支援 Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 及 Mozilla Thunderbird 的「垃圾郵件防護」保護。

4.3.1 自學垃圾郵件防護

「自學垃圾郵件防護」與上述貝氏過濾相關。隨著將個別郵件標記為垃圾郵件或非垃圾郵件，個別字的重要性亦隨之變更。因此，所分類的郵件越多 (標記為垃圾郵件或非垃圾郵件)，利用貝氏過濾取得的結果就越準確。

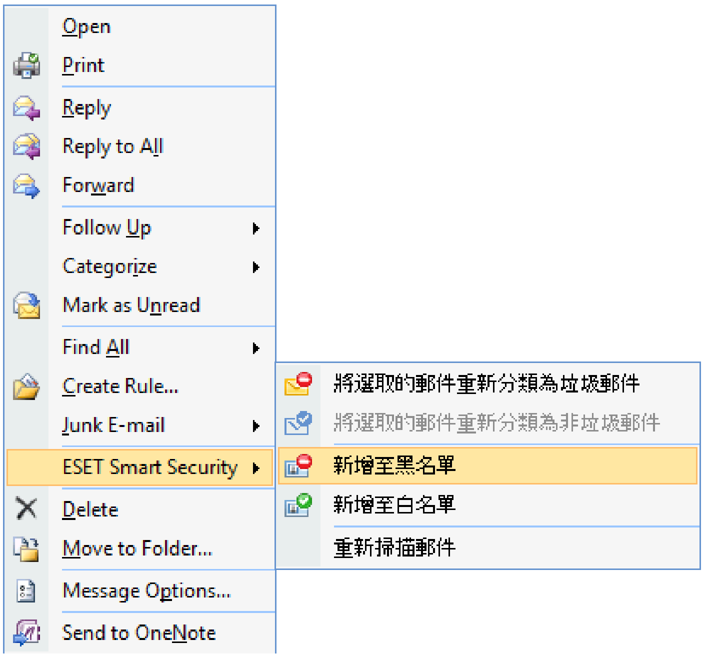
將已知位址新增到白名單，以排除對來自於這些位址的郵件進行過濾。

4.3.1.1 新增位址到白名單

若使用者與某些人員的通訊較為頻繁，可將這些人員的電子位址新增至「安全」位址的清單 (白名單)。這樣可確保來自於白名單位址的郵件始終不會分類為垃圾郵件。若要將新位址新增至白名單，請以滑鼠右鍵按一下特定的電子郵件並選取 [ESET Smart Security] 內容功能表選項下的 [**新增至白名單**]，或按一下電子郵件程式上半部 ESET Smart Security [垃圾郵件防護] 工具列中的 [**信任的位址**]。同樣，此程序也適用於垃圾郵件位址。如果在黑名單上列出電子郵件位址，則從此位址收到的每封電子郵件都會分類為垃圾郵件。

4.3.1.2 將郵件標記為垃圾郵件

在電子郵件用戶端中檢視的任何郵件都可以標記為垃圾郵件。若要這樣做，請使用內容功能表 (按一下滑鼠右鍵，然後按一下 [**ESET Smart Security**] > [**將選取的郵件重新分類為垃圾郵件**])，或從位於電子郵件用戶端中的 ESET Smart Security [垃圾郵件防護] 工具列按一下 [**垃圾郵件**]。



重新分類的郵件會自動移至 SPAM 資料夾，但是寄件者電子郵件位址不會新增至黑名單。同樣地，可將郵件分類為「非垃圾郵件」。如果將來自 [**垃圾電子郵件**] 資料夾的郵件分類為非垃圾郵件，則這些郵件會被移至原始資料夾。將郵件標記為非垃圾郵件不會自動將寄件者位址新增至「白名單」。

4.4 更新程式

為獲得 ESET Smart Security 所提供的最高安全等級，基本前提是要定期更新系統。「更新」模組可確保程式永遠處於最新狀態。您可透過兩種方式達成此目的 – 更新病毒資料庫及更新所有系統元件。

按一下 [**更新**]，可以找到目前更新狀態的相關資訊，包括病毒資料庫的目前版本及是否需要更新。此外，可以使用立即啟動更新處理程序的選項 ([**更新病毒資料庫**])，以及基本更新設定選項，例如存取 ESET 更新伺服器的使用者名稱及密碼。

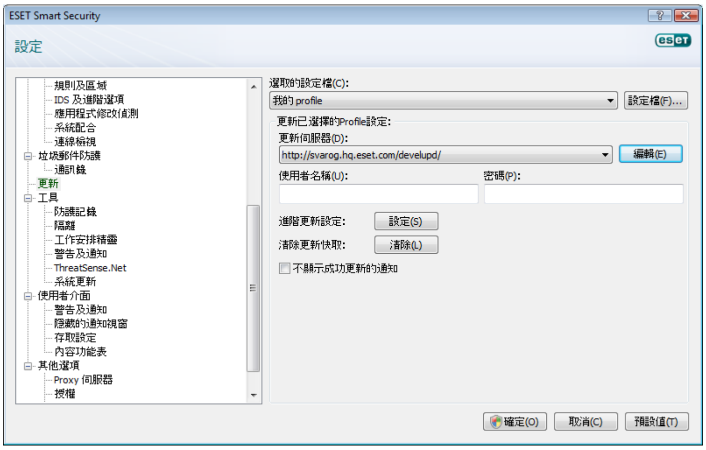
資訊視窗也包含上次成功更新的日期及時間，以及病毒資料庫號碼等詳細資料。此數字指示是連往 ESET 網站的有效連結，而網站中會列出特定更新中新增的所有簽章。

使用 [**登錄**] 連結開啟登錄表單，此表單會要求您使用新授權登錄 ESET，並於稍後將您的驗證資料傳遞到您的電子郵件。

附註：購買 ESET Smart Security 之後，ESET 會提供「使用者名稱」及「密碼」。

4.4.1 更新設定

更新設定區段指定更新來源資訊，如更新伺服器及這些伺服器的驗證資料。依預設，[**更新伺服器:**] 欄位會設為 [**選擇自動**]。此值可確保從具有最少網路流量負載的 ESET 伺服器自動下載更新檔案。您可從 [**更新**] 下的 [進階設定] (F5) 樹狀目錄，取得更新設定選項。



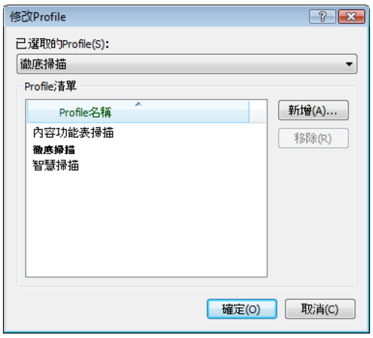
目前現有更新伺服器清單可透過 [**更新伺服器:**] 下拉式功能表存取。若要新增更新伺服器，請按一下 [**更新所選設定檔的設定**] 區段中的 [**編輯...**]，然後按一下 [**新增**] 按鈕。

更新伺服器的驗證由「**使用者名稱**」及「**密碼**」授與，在購買產品授權後，ESET 就會產生並傳送給使用者。

4.4.1.1 更新設定檔

您可針對不同更新配置，建立使用者定義的更新設定檔，以用於特定更新工作。建立不同更新設定檔對於行動使用者尤其實用，因為網際網路連線內容經常變更。行動使用者可修改更新工作，指定無法使用 [**我的設定檔**] 中指定的配置進行更新時，使用替代設定檔執行更新。

[**已選取的 Profile**] 下拉式功能表會顯示目前選取的設定檔。依預設，此項目設為 [**我的設定檔**]。若要建立新設定檔，請按一下 [**設定檔...**] 按鈕，然後按一下 [**新增...**] 按鈕，並輸入您自己的 [**設定檔名稱**]。建立新設定檔時，可以使用下列方式從現有設定檔中複製設定，也就是從 [**從設定檔複製設定:**] 下拉式功能表中進行選取。



您可以在設定檔設定內，指定程式要連線並下載更新的更新伺服器；您可使用可用伺服器清單中的任何伺服器，或新增伺服器。現有更新伺服器的清單可透過 [**更新伺服器:**] 下拉式功能表進行存取。若要新增更新伺服器，請按一下 [**更新已選擇的Profile設定**] 區段中的 [**編輯...**]，然後按一下 [新增] 按鈕。

4.4.1.2 進階更新設定

若要檢視 [**進階更新設定**]，請按一下 [**設定...**] 按鈕。進階更新設定選項包括 [**更新模式**]、[**HTTP Proxy**]、[**LAN**] 及 [**映像**] 的配置。

4.4.1.2.1 更新模式

[**更新模式**] 索引標籤包含程式元件更新的相關選項。

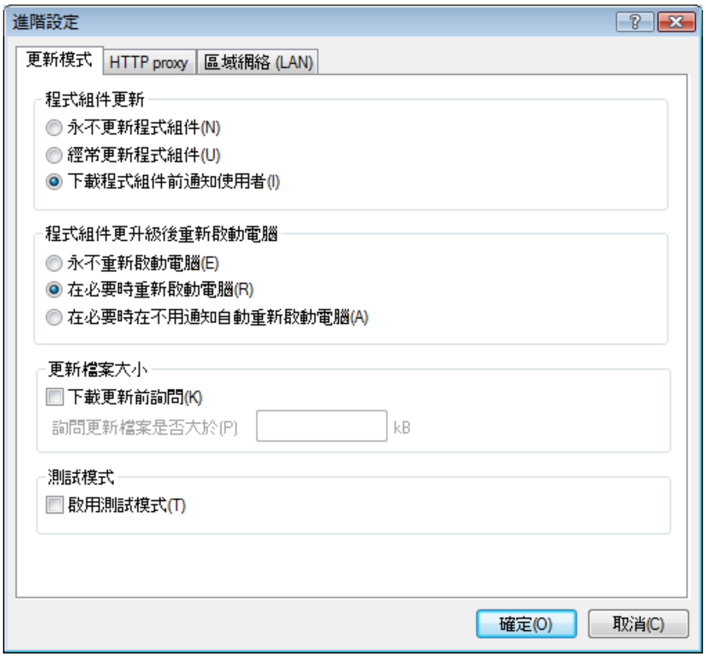
[**程式元件更新**] 區段中，有三個選項可用：

- **絕不更新程式元件**
- **經常更新程式組件**
- **下載程式元件前詢問**

選取 [**絕不更新程式元件**] 選項會確認 ESET 發佈新程式元件更新之後，不下載更新，且特定工作站上不會進行任何程式元件更新。[**經常更新程式組件**] 選項表示每次 ESET 更新伺服器上有新的更新可用時，都會執行程式元件更新，且該程式元件會升級為下載的版本。

選取第三個選項 [**下載程式元件前詢問**]，可確保程式會在有此類更新時，要求使用者確認是否下載程式元件更新。在此情況下，會顯示一對話視窗，其中包含可用程式元件更新的相關資訊，以及確認或拒絕的選項。如果確認，則會下載更新並安裝新的程式元件。

程式元件更新的預設選項為 [**下載程式元件前詢問**]。



安裝完程式元件更新之後必須重新啟動系統，所有模組的完整功能才能正常運作。[**程式元件升級後重新啟動**] 區段有三種選項可供選取：

- **絕不重新啟動電腦**
- **必要時重新啟動電腦**
- **必要時不通知即重新啟動電腦**

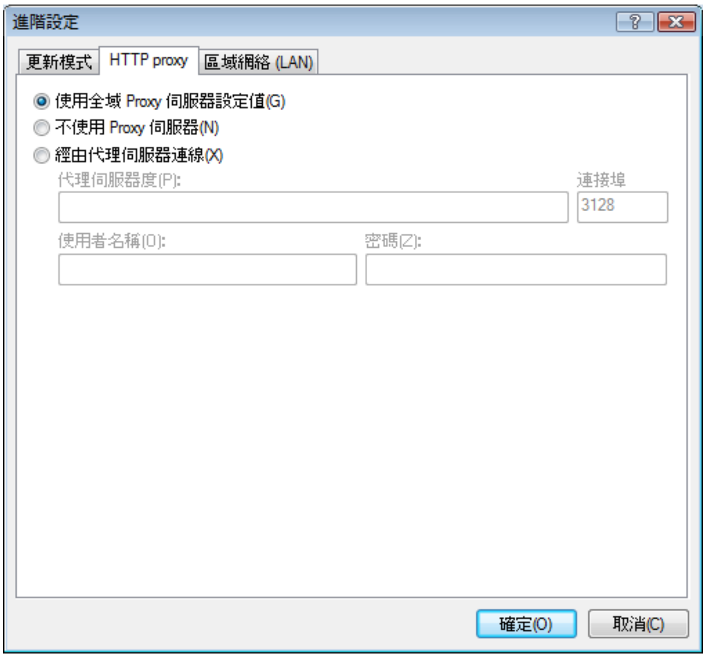
重新啟動的預設選項為 [**必要時重新啟動電腦**]。[**更新模式**] 索引標籤內，會根據要套用設定的個別不同工作站，提供不同的最適用程式元件更新選項。請注意，工作站與伺服器並不相同，例如，程式升級後自動重新啟動伺服器會導致嚴重損毀。

4.4.1.2.2 Proxy 伺服器

若要特定更新設定檔的 Proxy 伺服器設定選項：請按一下 [進階設定] (F5) 樹狀目錄中的 [**更新**]，然後按一下 [**進階更新設定**] 右側的 [**設定...**] 按鈕。按一下 [**HTTP Proxy**] 索引標籤，並選取下列三個選項之一：

- **使用全域 Proxy 伺服器設定值**
- **不使用 Proxy 伺服器**
- **經由代理伺服器連線** (連線內容定義的連線)

選取 [**使用全域 Proxy 伺服器設定值**] 選項，會使用已在 [進階設定] 樹狀目錄之 [**其他選項 > Proxy 伺服器**] 子目錄內指定的 Proxy 伺服器配置選項。



選取 [**不使用 Proxy 伺服器**] 選項，以明確定義不使用任何 Proxy 伺服器更新 ESET Smart Security。

如果要使用 Proxy 伺服器更新 ESET Smart Security，且該伺服器與全域設定 ([**其他選項 > Proxy 伺服器**]) 中指定的 Proxy 伺服器不同，則應選擇 [**經由代理伺服器連線**]　選項。如果是這樣的話，則應在此指定設定：[**Proxy 伺服器**] 位址、通訊 [**連接埠**]，以及 Proxy 伺服器的 [**使用者名稱**] 及 [**密碼**] (如果需要的話)。

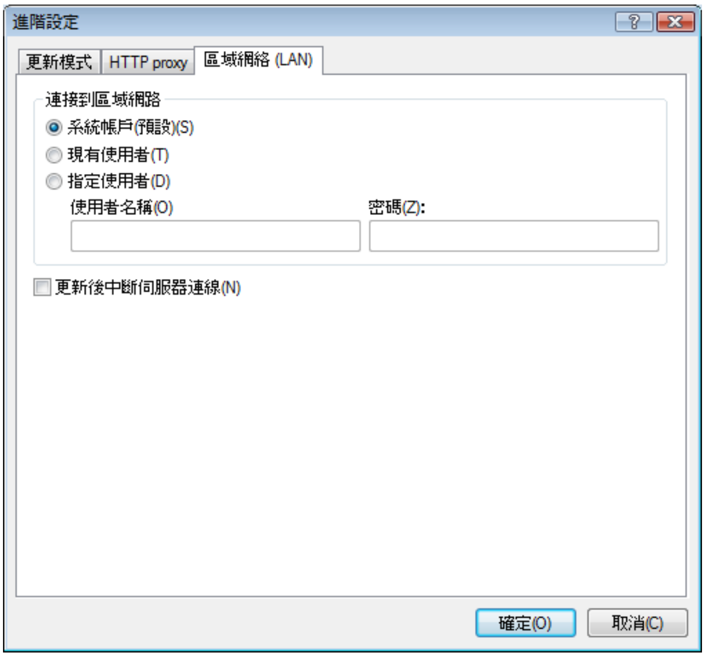
如果未全域設定 Proxy 伺服器設定，但 ESET Smart Security 將連接至 Proxy 伺服器進行更新，亦應選取此選項。

Proxy 伺服器的預設值為 [**使用全域 Proxy 伺服器設定值**]。

4.4.1.2.3　連線至 LAN

從使用 NT 型作業系統的本機伺服器更新時，依預設需驗證各網路連線。在大多數情況下，本機系統帳戶沒有足夠權限可存取 [映像] 資料夾 ([映像] 資料夾包含更新檔案的副本)。如果是這種情況，請在更新設定區段中輸入使用者名稱及密碼，或若使用程式進入更新伺服器 (映像)，則指定該程式的現有帳戶。

若要配置此類帳戶，請按一下 [**LAN**] 索引標籤。[**連接到區域網路**] 區段提供 [**系統帳戶**] (預設)、[**現有使用者**] 和 **指定使用者**] 等選項。



選取 [**系統帳戶**] 選項，以使用系統帳戶來驗證。通常，如果主要更新設定區段中未提供任何驗證資料，則不會執行驗證處理程序。

若要確保程式使用目前登入的使用者帳戶自我授權，請選取 [**現有使用者**]。此解決方案的缺點是如果目前沒有任何使用者登入，程式就無法連線至更新伺服器。

如果您希望程式使用特定使用者帳戶進行驗證，請選取 [**指定使用者**]。

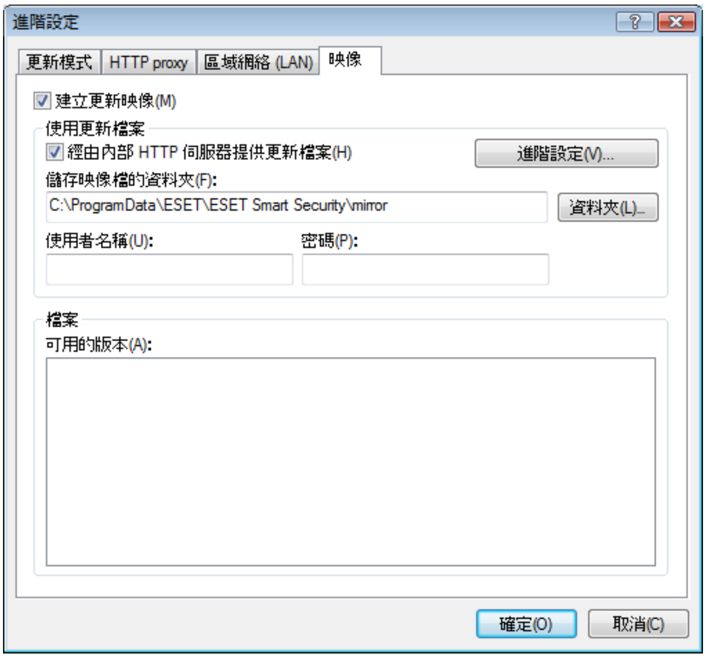
LAN 連線的預設選項為 [**系統帳戶**]。

警告：
啟用 [**現有使用者**] 或 [**指定使用者**] 時，若將程式身分變更為希望的使用者，則可能會發生錯誤。因此，我們建議將 LAN 驗證資料插入主要更新設定區段。請在此更新設定區段中，如下輸入驗證資料：網域名稱\使用者 (如果是工作群組，請輸入工作群組名稱\名稱) 及使用者密碼。當從本機伺服器 HTTP 版本更新時，不需要驗證。

4.4.1.2.4　建立更新副本 – 映像

ESET Smart Security Business Edition 可讓使用者建立更新檔案的副本，以更新網路中的其他工作站。從 [映像] 更新用戶端工作站可最佳化網路負載平衡，並節省網際網路連線頻寬。

本機伺服器 [映像] 的配置選項存取位置為 (在授權管理程式中新增有效的授權金鑰之後，位於 ESET Smart Security Business Edition 的 [進階設定] 區段中) [**進階更新設定：**] 區段 (若要存取此區段，請按 F5 並按一下 [進階設定] 樹狀目錄中的 [**更新**]。按一下 [**進階更新設定：**] 旁邊的 [**設定...**] 按鈕，並選取 [**映像**] 索引標籤)。



配置 [映像] 的第一步是勾選 [**建立更新映像**] 核取方塊。選取此選項會啟動其他 [映像配置] 選項，例如存取更新檔案的方式及映像檔案的更新路徑。

[映像]　啟動的方法詳述於下一章「存取映像的不同方法」中有詳細說明。目前有兩種基本方法可存取 [映像] - 將含有更新檔案的資料夾呈現為共用網路資料夾的 [映像]，或呈現為 HTTP 伺服器的 [映像]。

[**儲存映像檔案的資料夾**] 區段會定義儲存 [映像] 更新檔案的專用資料夾。按一下 [**資料夾...**] 以瀏覽本機電腦或共用網路資料夾上的所需資料夾。如果指定的資料夾需要授權，請在 [**使用者名稱**] 及 [**密碼**] 欄位中提供驗證資料。[使用者名稱] 及 [密碼] 的輸入格式應為「***網域/使用者***」或「***工作群組/使用者***」。請記得提供對應的密碼。

指定詳細 [映像] 配置時，您還可以指定要下載更新副本的語言版本。語言版本設定可從 [**檔案 > 可用的版本：**] 區段存取。

4.4.1.2.4.1 從映像更新

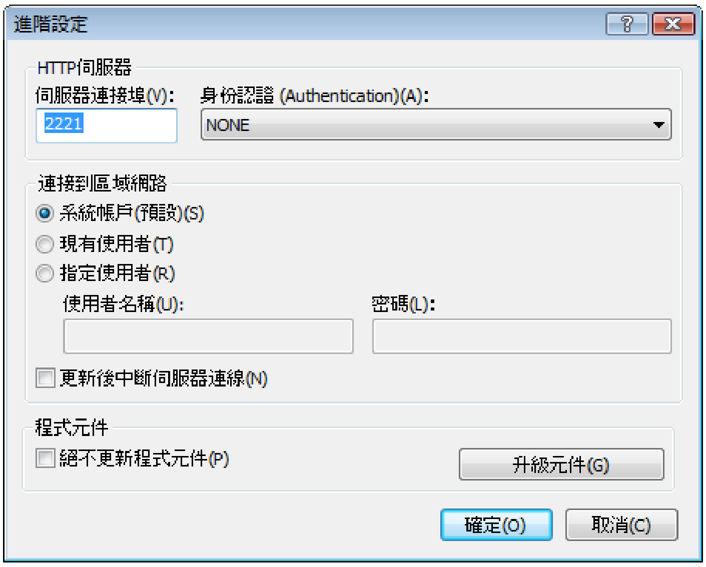
有兩種配置 [映像] 的基本方法 - 將含有更新檔案的資料夾呈現為共用網路資料夾的 [映像]，或呈現為 HTTP 伺服器的 [映像]。

使用內部 HTTP 伺服器存取映像

此配置為預設值，已指定於預先定義的程式配置中。若要允許使用 HTTP 伺服器存取 [映像]，請瀏覽至 [**進階更新設定**]（[**映像**] 索引標籤），並選取 [**建立更新映像**] 選項。

您可以在 [**映像**] 索引標籤的 [**進階設定**] 區段中，指定 HTTP 伺服器要監聽的 [**伺服器連接埠**]，以及 HTTP 伺服器所使用的 [**驗證**] 類型。依預設，[伺服器連接埠] 的值設為 **2221**。[**身份認證**] 選項定義存取更新檔案所使用的驗證方法。可用選項如下：**NONE**、**基本** 及 **NTLM**。選取 [**基本**] 以使用具有基本使用者名稱及密碼驗證的 base64 編碼。[**NTLM**] 選項提供使用安全編碼方法的編碼。而會使用共用更新檔案之工作站上建立的使用者進行驗證。預設值為 [**NONE**]，可授與無需驗證之更新檔案的存取權。

警告：
如果您希望允許透過 HTTP 伺服器存取更新檔案，則 [映像] 資料夾必須位於 ESET Smart Security 實例建立此資料夾的同一部電腦。



配置 [映像] 完成之後，請移至工作站並新增更新伺服器，格式為 **http://IP_address_of_your_server:2221**。若要執行此操作，請遵循以下步驟：

- 開啟 [**ESET Smart Security 進階設定**] 並按一下 [**更新**] 子目錄。
- 按一下 [**更新伺服器**] 下拉式功能表右側的 [**編輯...**]，並使用下列格式新增伺服器：http://您伺服器的 IP 位址：2221
- 從更新伺服器清單中選取此新增的伺服器。

透過系統共用存取映像

首先，請在本機或網路裝置上建立共用資料夾。建立 [映像] 的資料夾時，對於會將更新檔案儲存至資料夾的使用者，必須提供「寫入」權限，對於會從 [映像] 資料夾更新 ESET Smart Security 的使用者，應提供「讀取」權限。

接著請停用 [**經由內部 HTTP 伺服器提供更新檔案** 選項，在 [**進階更新設定**] 區段（[**映像**] 索引標籤）中設定 [映像] 的存取權。程式安裝套件中已預設啟用此選項。

如果共用資料夾位於網路中的另一部電腦，您必須指定驗證資料以存取其他電腦。若要指定驗證資料，請開啟 ESET Smart Security 的 [進階設定] (F5)，並按一下 [**更新**] 子目錄。按一下 [**設定...**] 按鈕，然後按一下 [**LAN**] 索引標籤。此設定與更新的設定相同，如「連線至 LAN」一章中所述。

[映像] 配置完成之後，繼續前往工作站，並將 \\UNC\PATH 設為更新伺服器。您可使用下列步驟完成此作業：

- 開啟 ESET Smart Security 的 [進階設定]，並按一下 [**更新**]
- 按一下 [更新伺服器] 旁邊的 [**編輯...**]，並使用 \\UNC\PATH 格式新增伺服器。
- 從更新伺服器清單中選取此新增的伺服器

附註：
若要正常發揮功能，[映像] 資料夾的路徑必須指定為 UNC 路徑。從對應磁碟機更新可能無法運作。

4.4.1.2.4.2 疑難排解映像更新問題

根據用來存取 [映像] 資料夾方式不同，可能會發生各種類型的問題。在大部分情況下，若從 [映像] 伺服器更新期間發生問題，原因可能是下列一或多項：[映像] 資料夾選項的指定不正確、對 [映像] 資料夾資料的驗證不正確、對嘗試從 [映像] 下載更新檔案之本機工作站的配置不正確，或上述原因的組合。這裡提供了從 [映像] 更新期間最常可能發生之問題的概觀。

- **連接至映像伺服器時，ESET Smart Security 報告錯誤** - 可能的原因是本機工作站要下載更新的來源更新伺服器（映像資料夾的網路路徑）的指定有誤。若要驗證資料夾，請按一下 Windows 的 [**開始**] 功能表、按一下 [**執行**]，插入資料夾名稱並按一下 [**確定**]。螢幕上應會顯示資料夾內容。
- **ESET Smart Security 需要使用者名稱及密碼** – 可能的原因是在更新區段中輸入的驗證資料（使用者名稱及密碼）不正確。「使用者名稱」及「密碼」用於授與更新伺服器（程式更新位置）的存取權。請確定驗證資料正確，且以正確的格式輸入。例如，[***網域/使用者名稱***] 或 [***工作群組/使用者名稱***]，以及對應的 [密碼]。請注意，若 [映像] 伺服器的存取權設為 [每個人]，並不代表任何使用者都具有存取權。[每個人] 不表示任何未獲授權的使用者，僅表示所有網域使用者都可以存取資料夾。因此，若資料夾的存取權設為 [每個人]，還是必須在更新設定區段中輸入網域使用者名稱及密碼。
- **連接至映像伺服器時，ESET Smart Security 報告錯誤** – 封鎖定義用於存取 [映像] HTTP 版本之連接埠的通訊。

4.4.2 如何建立更新工作

您可使用下列方式手動觸發更新：按一下主要功能表中的 [**更新**] 之後，在顯示的資訊視窗中按一下 [**更新病毒資料庫**]**。**

亦可排程執行更新工作 – 若要配置排定工作，請按一下 [**工具 > 工作安排精靈**]。依預設，會在 ESET Smart Security 中啟動下列工作：

- **定期自動更新**
- **撥號連線後自動更新**
- **使用者登入後自動更新**

上述各個更新工作都可以修改，以滿足您的需求。除了預設更新工作之外，您亦可利用使用者定義的配置來建立新的更新工作。如需建立及配置更新工作的詳細資料，請參閱「工作安排精靈」一章。

4.5 工作安排精靈

如果啟動 ESET Smart Security 中的 [進階] 模式，即可使用工作安排精靈。您可在 **[工具]** 下方的 ESET Smart Security 主要功能表中找到 **[工作安排精靈]**。工作安排精靈包含所有排定工作及其配置內容(例如預先定義的日期、時間、使用的掃描設定檔) 的摘要清單。

依預設，下列排定工作會顯示在 **[工作安排精靈]** 中：

- **定期自動更新**
- **撥號連線後自動更新**
- **使用者登入後自動更新**
- **使用者登入後自動啟動檔案檢查**
- **成功更新病毒資料庫後自動啟動檔案檢查**

若要編輯 (預設及使用者定義的) 現有排定工作的配置，請在工作上按一下滑鼠右鍵並按一下 **[編輯...]**，或選取想要修改的所需工作並按一下 **[編輯...]** 按鈕。

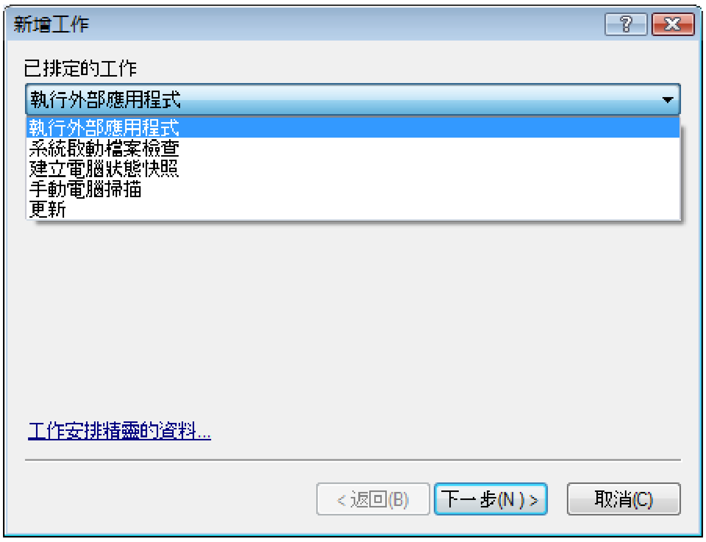
4.5.1 排定工作的目的

工作安排精靈使用預先定義的配置與內容，管理及啟動排定工作。配置及內容包含資訊，例如日期與事件，以及工作執行期間要使用的指定設定檔。

4.5.2 建立新工作

若要在 [工作安排精靈] 中建立新工作，請按一下 **[新增...]** 按鈕，或按一下滑鼠右鍵並從內容功能表中選取 **[新增...]**。有五種類型的排定工作可用：

- **執行外部應用程式**
- **防護記錄維護**
- **系統啟動檔案檢查**
- **手動電腦掃描**
- **更新**



由於 **[手動電腦掃描]** 及 **[更新]** 是最常用的排定工作，我們將解釋如何新增更新工作。

從 **[已排定的工作：]** 下拉式功能表，選取 [-更新]**。**按 **[下一步]** 並在 **[工作名稱：]** 欄位中輸入工作的 名稱。選取工作的頻率。可用選項如下：**一次**、**重複**、**每日**、**每星期**和**事件觸發**。系統會根據選取的頻率，提示您不同的更新參數。接著，定義排程期間無法執行或完成工作時要採取的處理方法。可用的三個選項如下：

- **等到下一個排定的時間**
- **盡快執行工作**
- **如果距離上次執行工作的時間超過指定的時間間隔，則立即執行工作** (可以使用 **[工作時間間隔]** 捲動方塊立即定義間隔)

在下一步中，會顯示具有目前排程工作資訊的摘要視窗；應會自動啟用 **[以特定參數執行工作]** 選項。按一下 **[完成]** 按鈕。

螢幕上會顯示對話視窗，讓您選取要用於排定工作的設定檔。您可在此指定主要設定檔及替代設定檔 (當工作無法以主要設定檔完成時使用)。按一下 **[更新設定檔]** 視窗中的 **[確定]** 來確認。新排定工作將新增至目前排定工作清單。

4.6 隔離

隔離的主要工作是安全地儲存受感染檔案。對於無法清除、無法安全刪除或不建議刪除的檔案，或者 ESET Smart Security 錯誤偵測到的檔案，應該予以隔離。

使用者可以選擇隔離任何想要隔離的檔案。如果檔案運作狀況有異，但防毒掃描器沒有偵測到，則建議進行隔離。您可將隔離的檔案提交至 ESET 病毒實驗室進行分析。

您可在表格中檢視儲存於隔離資料夾的檔案，表格中會顯示隔離的日期與時間、受感染檔案原始位置的路徑、大小 (以位元組為單位)、原因 (**由使用者新增...**)，以及威脅數量 (例如，包含多個入侵的壓縮檔)。

4.6.1 隔離檔案

程式會自動隔離刪除的檔案 (如果您尚未在警告視窗中取消此選項)。如果需要，您可以按一下 [**隔離...**] 按鈕，手動隔離任何可疑檔案。如果是這種情況，則原始檔案不會從其原始位置移除。亦可使用內容功能表達到此目的 – 在隔離區視窗中按一下滑鼠右鍵，並選取 [**新增...**]

4.6.2 從隔離區還原

隔離的檔案還可還原至其原始位置。使用 [**還原**] 功能可達到此目的；在隔離區視窗中的特定檔案上按一下滑鼠右鍵，即可從內容功能表使用此功能。內容功能表還提供 [**還原到**] 選項，可讓您將檔案還原到其原始刪除位置外的其他位置。

附註：
如果程式錯誤地隔離了無害檔案，請在還原後從掃描中排除此檔案，並將該檔案傳送至「ESET 客戶關懷」。

4.6.3 從隔離區提交檔案

如果您已隔離程式未偵測到的可疑檔案，或有檔案被誤判為受到感染 (例如以代碼的啟發式分析) 而被隔離，請將檔案傳送至 ESET 病毒實驗室。若要從隔離區提交檔案，請在檔案上按一下滑鼠右鍵，並從內容功能表選取 [**提交檔案以供分析**]。

4.7 防護記錄檔案

「防護記錄檔案」包含所有已發生之重要程式事件的相關資訊，並提供偵測到之威脅的概觀。在系統分析、威脅偵測及疑難排解方面，防護記錄都是一項很重要的工具。防護記錄會主動在背景中執行，不需使用者互動。系統會根據目前的防護記錄冗贅設定來記錄資訊。您可以直接從 ESET Smart Security 環境檢視文字訊息及防護記錄，以及保存防護記錄。

從 ESET Smart Security 主視窗中按一下 [**工具 > 防護記錄檔案**]，可以存取防護記錄檔案。選取所需的防護記錄類型，方法是使用視窗頂端的 [**防護記錄：**] 下拉式功能表。可用的防護記錄如下：

1. **偵測到威脅** – 使用此選項，可檢視與偵測入侵相關之事件的所有資訊。

2. **事件** – 此選項旨在供系統管理員及使用者解決問題。ESET Smart Security 執行的所有重要處理方法都會記錄在「事件」防護記錄中。

3. **手動電腦掃描** – 所有已完成掃描的結果都會顯示在此視窗中。按兩下任何項目，以檢視各手動掃描的詳細資料。

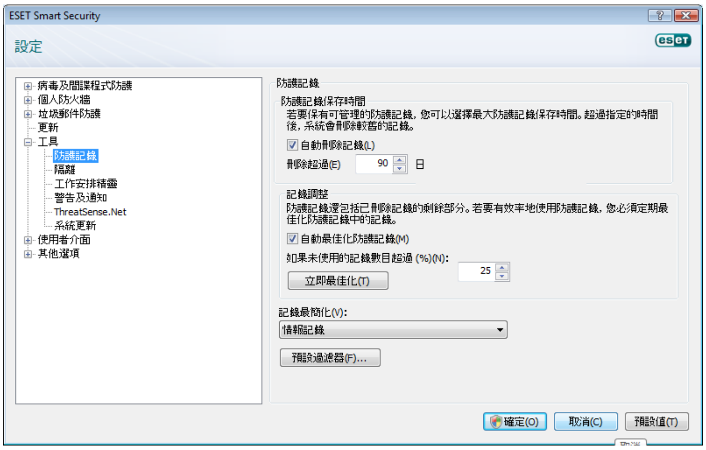
4. **ESET 個人防火牆日誌** – 包含 [個人防火牆] 所偵測以及與其相關的所有事實記錄。防火牆日誌的分析有助於即時偵測到侵入系統的企圖，以防止未經授權的人存取您的系統。

在每個區段中，選取項目並按一下 [**複製**] 按鈕，可將顯示的資訊直接複製到剪貼簿。若要選取多個項目，可使用 CTRL 及 SHIFT 鍵。

4.7.1 防護記錄維護

您可從主程式視窗存取 ESET Smart Security 的記錄配置。按一下 [**設定 > 進入完整的進階設定樹狀目錄... > 工具 > 防護記錄檔案**]。您可以指定下列用於防護記錄檔案的選項：

- **自動刪除記錄**：自動刪除超過指定天數的防護記錄項目
- **自動最佳化防護記錄**：若未使用的記錄超出指定的百分比，則自動重組防護記錄檔案
- **記錄最簡化**：指定記錄冗贅等級。可用的選項：
  - **嚴重錯誤** – 僅記錄嚴重錯誤 (啟動 [防毒保護]、[個人防火牆] 等發生的錯誤)
  - **錯誤** – 只記錄「下載檔案時發生錯誤」訊息及嚴重錯誤
  - **警告** – 記錄嚴重錯誤及警告訊息
  - **情報記錄** – 記錄包含成功更新訊息及所有上述記錄的資訊性訊息
  - **診斷記錄** – 記錄程式微調所需的資訊及所有上述記錄



4.8 使用者介面

您可根據需求修改 ESET Smart Security 中的使用者介面配置選項，以調整工作環境。這些配置選項可從 ESET Smart Security 之 [進階設定] 樹狀目錄的 [**使用者介面**] 子目錄中存取。

[**使用者介面元素**] 區段可讓使用者切換至「進階」模式 (如果需要的話)。[進階模式] 會顯示 ESET Smart Security 的詳細設定及其他控制項。

如果圖形元素使電腦的效能變慢或導致其他問題，則應停用 [**圖形使用者介面**] 選項。對於視覺障礙的使用者而言，可能也需要停用圖形介面，因為這可能會與用於讀出螢幕文字的特殊應用程式相衝突。

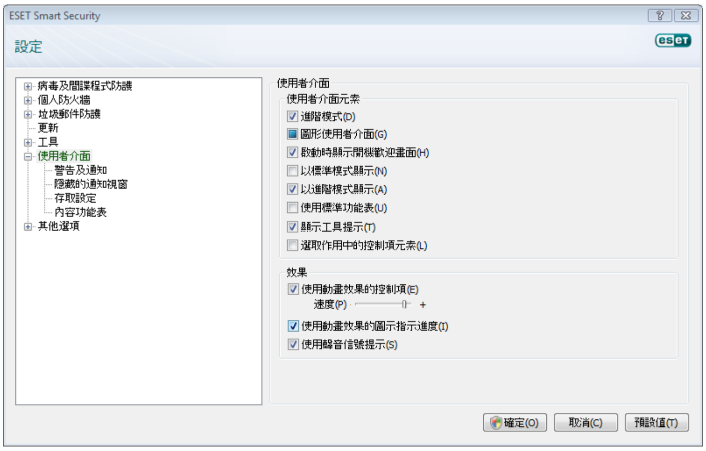
如果您要停用 ESET Smart Security 開頭顯示畫面，請停用 [**啟動時顯示開機歡迎畫面**] 選項。

ESET Smart Security 主要程式視窗頂端的 [標準] 功能表，會根據 [**使用標準功能表**] 選項啟動或停用。

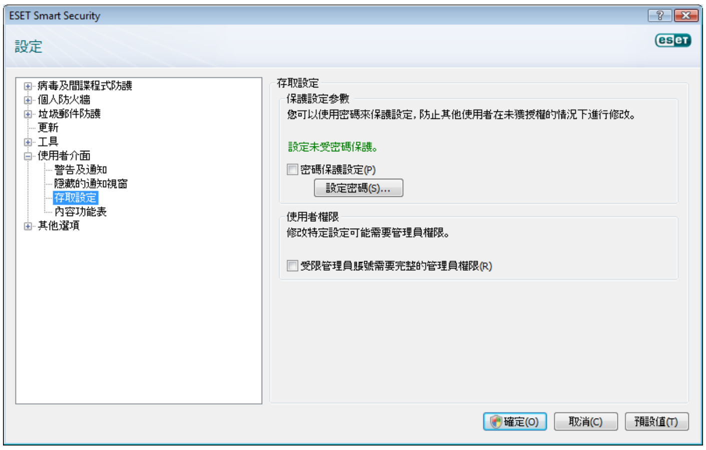
如果啟用了 [**顯示工具提示**] 選項，則將游標置於選項上時會顯示選項的簡短說明。[**選取作用中的控制項元素**] 選項會造成系統強調顯示目前在滑鼠游標作用中區域下的任何元素。滑鼠點選後會啟動強調顯示的元素。

若要降低或提高動畫效果的速度，請選取 [**使用動畫效果的控制項**] 選項，並將 [**速度**] 滑桿移到左側或右側。

若要使用動畫效果的圖示，以顯示各種作業的進度，請勾選 [**使用動畫效果的圖示...**] 核取方塊。如果您想要程式在發生重要事件時發出聲音警告，請選取 [**使用聲音信號提示**] 選項。



[**使用者介面**] 功能還包括使用密碼保護 ESET Smart Security 設定參數的選項。此選項位於 [**使用者介面**] 下的 [**設定保護**] 子功能表。為了提供系統最大的安全性，請務必正確地配置程式。未獲授權的修改可能會導致重要資料遺失。若要設定密碼以保護設定參數，請按一下 [**輸入密碼...**]



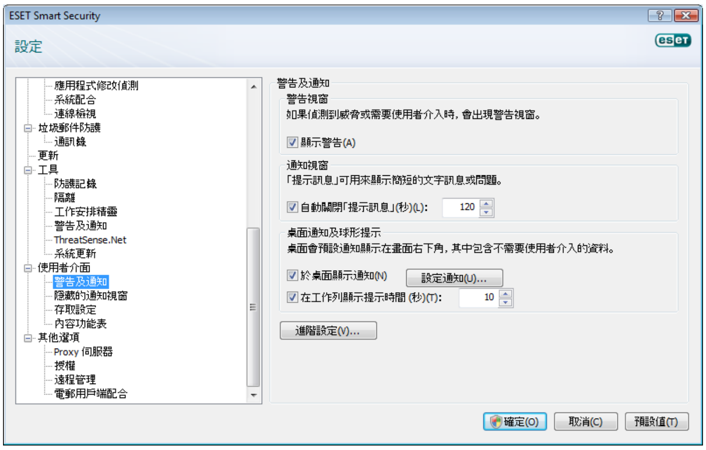
4.8.1 警告及通知

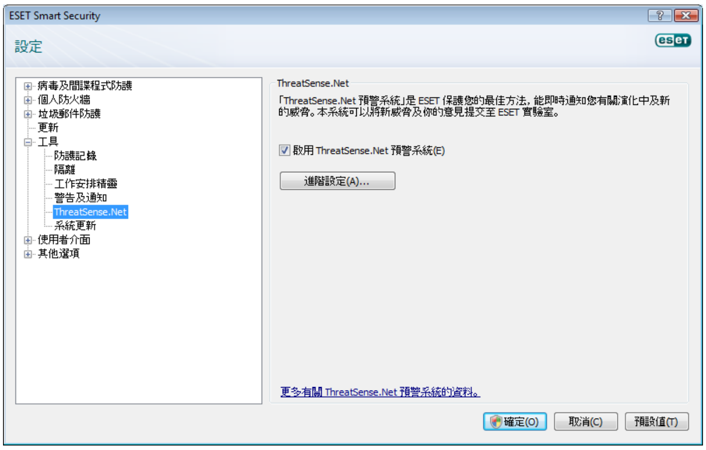
[**使用者介面**] 下的 [**警告及通知設定**] 區段，可讓您配置在 ESET Smart Security 4 中如何處理威脅警告及系統通知。

第一個項目是 [**顯示警告**]。停用此選項會取消所有警告視窗，僅適用於某些特定情況。對於大部分使用者而言，建議保留此選項的預設值 (啟用)。

若要在一段時間之後自動關閉快顯視窗，請選取 [**自動關閉提示訊息 (秒)**] 選項。如果使用者未手動關閉視窗，則指定時間到達時會自動關閉警告視窗。

桌面通知及球形提示僅為資訊性，不需要也不提供使用者互動。這會顯示在畫面右下角的通知區域中。若要啟動顯示桌面通知，請選取 [**於桌面顯示通知**] 選項。按一下 [**設定通知...**] 按鈕可以修改更多詳細選項，如通知顯示時間及視窗透明度。若要預覽通知的行為，請按一下 [**預覽**] 按鈕。若要配置球形提示顯示的持續時間，請勾選 [**在工作列顯示提示時間 (秒)**] 選項。





按一下 [**進階設定...**] 以進入其他 [**警告及通知**] 設定選項，包括 [**只顯示需要使用者互動的通知**]。您可以使用此選項，開啟/關閉顯示不需要使用者互動的警告及通知。選取 [只顯示在全螢幕模式中執行應用程式時需要使用者介入的通知]，以隱藏所有無互動的通知。您可以從 [最簡化要顯示的事件] 下拉式功能表中，選取要顯示之警告及通知的起始嚴重性等級。

此區段的最後一個功能，是在多個使用者環境中指定通知的位址。[**在多個使用者的系統中，在此使用者的畫面中顯示通知：**] 欄位可讓使用者定義從 ESET Smart Security 4 接收重要通知的人員。通常是系統或網路管理員。如果將所有系統通知都傳送給管理員，則此選項特別適用於終端機伺服器。

4.9 ThreatSense.Net

「ThreatSense.Net 預早警告系統」這項工具，可保持 ESET 立即並持續得到新入侵通知。雙向「ThreatSense.Net 預早警告系統」的單純目的，就是改善提供給您的防護。確保我們能儘快看到新威脅的最佳方式為「鏈結」儘可能多的客戶，並將它們用作我們的「威脅斥候」。有兩個選項：

- 您可以決定不啟用「ThreatSense.Net 預早警告系統」。您不會遺失軟體中的任何功能，且仍會得到我們能夠提供的最佳防護。

- 您可以配置「預早警告系統」，以使用單一檔案提交新威脅與包含新威脅代碼位置的匿名資訊。此檔案會傳送至 ESET 進行詳細分析。研究這些威脅可協助 ESET 更新其威脅偵測能力。「ThreatSense.Net 預早警告系統」會收集與新偵測到之威脅相關的電腦資訊。這些資訊可能包括出現威脅的檔案範例或副本、該檔案路徑、檔案名稱、日期與時間資訊、威脅出現在電腦上的程序，以及電腦作業系統的相關資訊。部分此資訊可能包括電腦使用者的個人資訊，如目錄路徑中的使用者名稱等。

雖然偶爾有可能將您及您電腦相關資訊洩露給 ESET 威脅實驗室，但此資訊僅用於協助我們對新威脅立即作出反應，除此之外不作其他任何用途。

依預設，ESET Smart Security 設定為先詢問，再將可疑檔案提交至 ESET 威脅實驗室進行詳細分析。請注意，若在 .doc 或 .xls 等特定副檔名的檔案中偵測到威脅，會一律排除不予傳送。若您或貴組織不希望傳送特殊檔案，亦可新增其他副檔名。

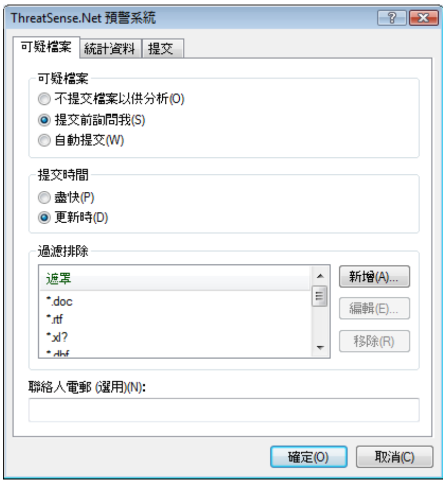
您可從 [進階設定] 樹狀目錄中的 [**工具 > ThreatSense.Net**] 下，存取 ThreatSense.Net 設定。勾選 [**啟用 ThreatSense.Net 預早警告系統**] 核取方塊。這可讓您啟動該系統，然後按一下 [**進階設定...**] 按鈕。

4.9.1 可疑檔案

[**可疑檔案**] 索引標籤可讓您配置將威脅提交至 ESET 實驗室進行分析的方法。

如果您發現可疑的檔案，可將其提交至我們的病毒實驗室進行分析。若檔案經證實為惡意的應用程式，會將其偵測功能新增至下一版的病毒資料庫更新。

檔案提交可設為自動執行而無需詢問。如果選取此選項，則會在背景中傳送可疑檔案。如果要知道已傳送哪些檔案以供分析並確認提交，請選取 [**提交前詢問我**] 選項。



如果不想提交任何檔案，請選取 [**不提交檔案以供分析**]。請注意，不提交檔案以供分析不會影響將統計資訊提交至 ESET。統計資訊配置於其本身的設定區段，如下一章中所述。

提交時間
可疑檔案會儘快傳送到 ESET 實驗室進行分析。如果有永久網際網路連線可用，建議使用此選項，就會儘快傳遞可疑檔案。另一個選項是**更新時**提交可疑檔案。如果選取此選項，則會收集可疑檔案並在更新期間將其上傳至「預早警告系統」伺服器。

排除過濾
並非所有檔案都必須提交以供分析。[排除過濾] 可讓您從排除特定檔案/資料夾不予提交。例如，您可使用此選項，排除可能包含潛在機密資訊的檔案，例如文件或試算表。依預設，最常用的檔案類型均會被排除在外 (Microsoft Office、OpenOffice)。如果需要，可以展開已排除檔案的清單。

聯絡人電郵
連絡人電子郵件會與可疑檔案一併傳送到 ESET，以在需要所提交檔案的進一步資訊以供分析時連絡您。請注意，除非需要更多資訊，否則您將不會收到 ESET 的任何回應。

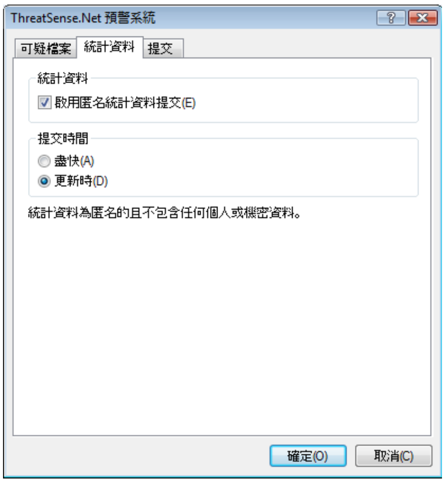
4.9.2 統計資料

「ThreatSense.Net預早警告系統」會收集與新偵測到之威脅相關的電腦匿名資訊。此資訊可包括入侵名稱、偵測日期及時間、ESET Smart Security 版本、電腦作業系統版本，以及位置設定。統計資料通常一天會傳遞到 ESET 伺服器一或兩次。

提交的統計套件範例：

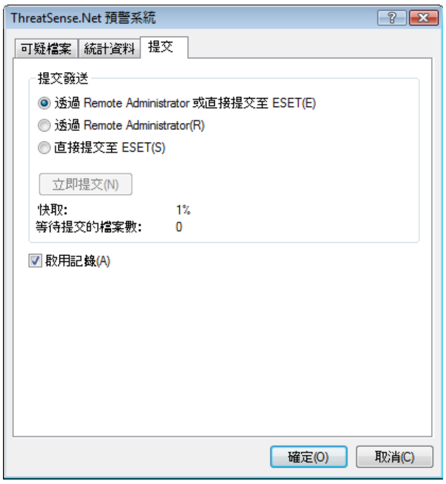
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1463[1].exe
```

提交時間
您可以在［**提交時間**］區段中，定義何時提交統計資訊。如果您選擇［**盡快**］提交，則統計資訊在建立之後會立即傳送。此設定適用於有永久網際網路連線可用時。如果選取［**更新時**］，則會保留統計資訊，並於下次更新時一起提交。



4.9.3 提交

您可在此區段中，選擇透過 ESET Remote Administrator 或直接將檔案及統計資訊提交至 ESET。如果要確定將可疑檔案及統計資訊傳遞至 ESET，請選取［**透過 Remote Administrator 或直接提交至 ESET**］選項。如果選取此選項，則會以所有可用的方法提交檔案及統計資料。[透過 Remote Administrator 提交可疑檔案] 會將檔案及統計資料提交至遠端管理伺服器，這可確保隨後提交至 ESET 病毒實驗室。如果選取 [**直接提交至 ESET**] 選項，則會將所有可疑檔案及統計資訊直接從程式傳送至 ESET 病毒實驗室。



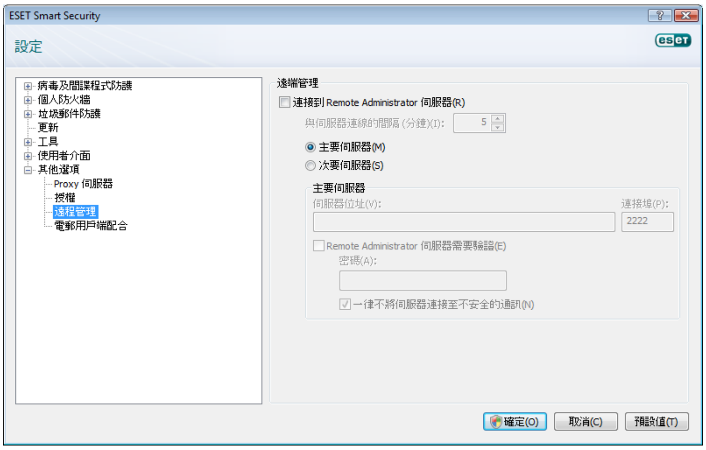
若有檔案等待提交，則此設定視窗中的［**立即提交**］按鈕會啟動。如果您要立即提交檔案及統計資訊，請按一下此按鈕。

勾選［**啟用記錄**］核取方塊，以記錄所提交的檔案及統計資訊。每次提交可疑檔案或統計資訊之後，都會在事件防護記錄中建立項目。

4.10 遠端管理

遠端管理是功能強大的工具，可維護安全原則及取得網路內整體安全管理的概觀。尤其適用於較大型網路。「遠端管理」不僅可提高安全等級，而且易於在用戶端工作站的 ESET Smart Security 管理中使用。

可您可在主要 ESET Smart Security 程式視窗中使用 [遠端管理設定] 選項。按一下 [**設定 > 進入完整的進階設定樹狀目錄... > 其他選項 > 遠端管理**]。



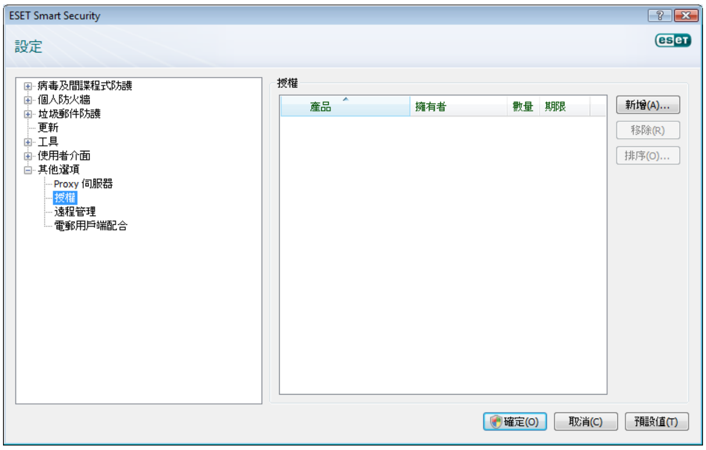
[設定] 視窗可讓您勾選［**連接到 Remote Administrator 伺服器**］核取方塊，啟動遠端管理模式。接著即可存取如下所述的其他選項：

- **伺服器位址** – 安裝遠端管理伺服器的伺服器網路位址。
- **連接埠** – 此欄位包含用於連線之預先定義的伺服器連接埠。建議您保留預先定義的連接埠設定 2222。
- **與伺服器連線的間隔（分鐘）** – 這會指定 ESET Smart Security 連接至 ERA 伺服器以傳出資料的頻率。也就是說，會以此處定義的時間間隔傳送資訊。如果設為 0，則提交資訊的間隔為 5 秒。
- **Remote Administrator 需要驗證** – 可讓您輸入連接至遠端管理伺服器的密碼（如果需要的話）。

按一下 [**確定**] 以確認變更並套用設定。ESET Smart Security 將會使用這些設定來連接至遠端伺服器。

4.11 授權

[**授權**] 子目錄可讓您管理 ESET Smart Security 及其他 ESET 產品 (如 ESET Remote Administrator、ESET NOD32 for Microsoft Exchange 等) 的授權金鑰。購買之後，您會連同「使用者名稱」及「密碼」一起收到授權金鑰。若要 [**新增/移除**] 授權金鑰，請按一下授權管理程式視窗中的對應按鈕。您可從 [進階設定] 樹狀目錄中的 [**其他選項 > 授權**] 下存取授權管理程式。



授權金鑰是是文字檔案，其中記載所購買產品的相關資訊：擁有者、授權數量及到期日。

授權管理程式視窗可讓使用者使用 [**新增...**] 按鈕，上傳及檢視授權金鑰的內容，這些資訊都會顯示在管理程式中。若要從清單刪除授權檔案，請按一下 [**移除**]。

如果授權金鑰已到期且您想要續訂，請按一下 [**訂購...**] 按鈕，就會將您重新導向至我們的線上商店。

5. 進階使用者

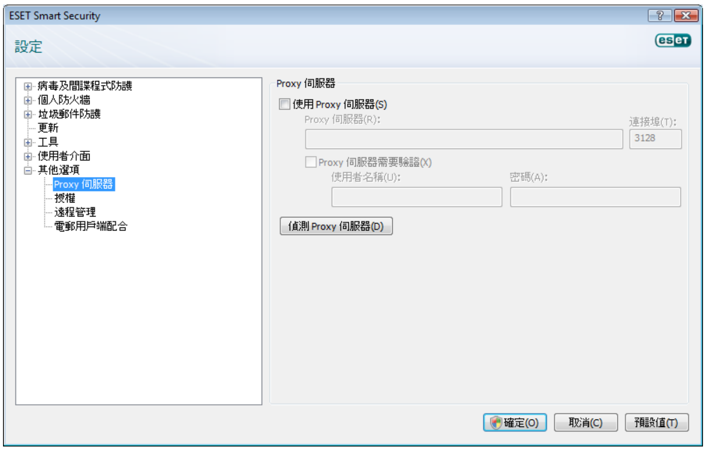
本章說明的 ESET Smart Security 功能，適用於較進階的使用者。只有在 [進階] 模式中才可存取這些功能的設定選項。若要切換至 [進階] 模式，請按一下主要程式視窗左下角的 [**切換進階模式**]，或者在鍵盤上按 CTRL + M 鍵。

5.1 Proxy 伺服器設定

在 ESET Smart Security 中，可以在 [進階設定] 樹狀結構內的兩個不同區段中進行 Proxy 伺服器設定。

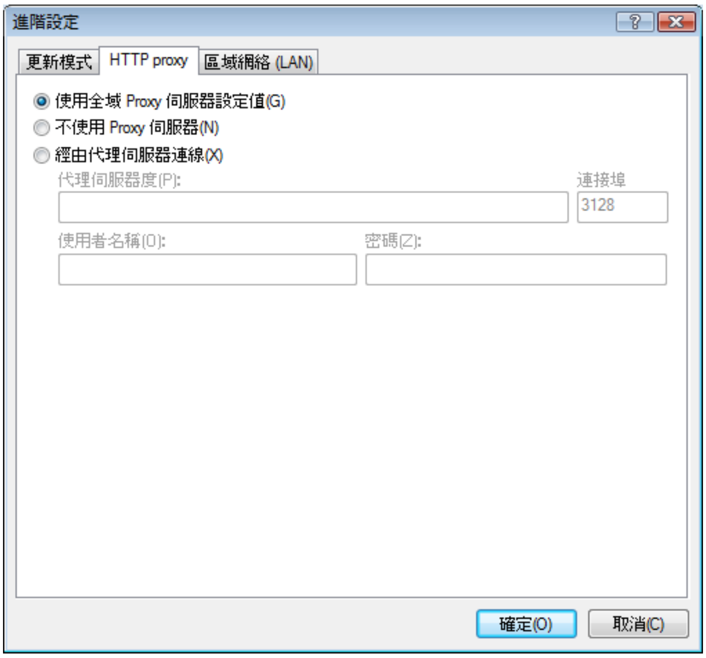
首先，可以在 [**其他選項 > Proxy 伺服器**] 下配置 Proxy 伺服器設定。在這個等級指定 Proxy 伺服器，會定義所有 ESET Smart Security 的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡設定的參數。

若要指定此等級的 Proxy 伺服器設定，請勾選 [**使用 Proxy 伺服器**] 核取方塊，然後將 Proxy 伺服器的位址輸入 [**Proxy 伺服器：**] 欄位中，同時輸入 Proxy 伺服器的 [**連接埠**] 號碼。



如果與 Proxy 伺服器之間的通訊需要驗證，請勾選 [**Proxy 伺服器需要驗證**] 核取方塊，並將有效的 [**使用者名稱**] 及 [**密碼**] 輸入各自的欄位中。按一下 [**偵測 Proxy 伺服器**] 按鈕，以自動偵測並插入 Proxy 伺服器設定。這樣會複製 Internet Explorer 中指定的參數。請注意，此功能不會擷取驗證資料 (「使用者名稱」及「密碼」)，這些資料必須由使用者提供。

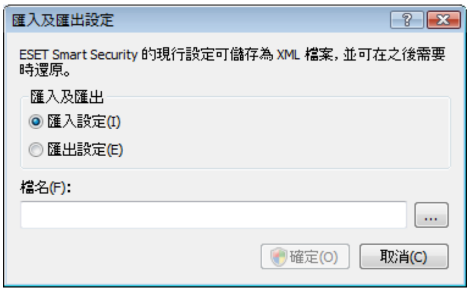
亦可在 [**進階更新設定**] ([進階設定] 樹狀目錄的 [**更新**] 子目錄) 中建立 Proxy 伺服器設定。此設定適用於特定的更新設定檔，且建議用於筆記型電腦，因為這類電腦經常會從不同的位置接收到病毒資料庫更新。如需此設定的相關資訊，請參閱第 4.4 節「更新程式」。



5.2 匯出/匯入設定

您可在 [**設定**] 下的 [進階] 模式中，匯出及匯入 ESET Smart Security 的目前配置。

匯出及匯入都使用 .xml 檔案類型。如果您 (因各種原因) 必須備份 ESET Smart Security 目前配置以供稍後使用，則匯出及匯入功能非常實用。對於希望在多系統上使用 ESET Smart Security 偏好配置的人員，應該也會喜愛匯出設定選項，因為僅需匯入 .xml 檔案即可達成。



5.2.1 匯出設定

匯出配置很簡單。如果您想要儲存 ESET Smart Security 目前配置，請按一下 [**設定 > 匯入及匯出設定...**]。選取 [**匯出設定**] 選項，並輸入配置檔案的名稱。使用瀏覽器，選取您希望在電腦上儲存配置檔案的位置。

5.2.2 匯入設定

匯入配置的步驟非常類似。同樣的，選取 [**匯入及匯出設定**]，然後選取 [**匯入設定**] 選項。按一下 [**...**] 按鈕，瀏覽至您希望匯入的配置檔案。

5.3 指令列

您可透過手動 (使用 ecls 指令) 或使用批次 (bat) 檔的方式，以指令列啟動 ESET Smart Security 的防毒模組。

從指令列執行手動掃描器時，可以使用下列參數及切換參數：

一般選項：

– help	顯示說明並結束
– version	顯示版本資訊並結束
– base-dir = FOLDER	從目的資料夾載入模組
– quar-dir = FOLDER	隔離目的資料夾
– aind	顯示活動指示器

目標：

– files	掃描檔案 (預設值)
– no-files	不掃描檔案
– boots	掃描開機磁區 (預設值)
– no-boots	不掃描開機磁區
– arch	掃描壓縮檔 (預設值)
– no-arch	不掃描壓縮檔
– max-archive-level = LEVEL	將檔案層度等級最大層數設為幾
– scan-timeout = LIMIT	將掃描壓縮檔的時間上限設定為限制秒。如果掃描時間達到此限制，則會停止掃描壓縮檔，並繼續掃描下一個檔案
– max-arch-size=SIZE	僅掃描壓縮檔中的前幾個位元組 (預設值 0 = 無限制)
– mail	掃描電子郵件檔案
– no-mail	不掃描電子郵件檔案
– sfx	掃描自我解壓縮檔
– no-sfx	不掃描自我解壓縮檔
– rtp	掃描運行時間壓縮器
– no-rtp	不掃描運行時間壓縮器
– exclude = FOLDER	從掃描中排除目的資料夾
– subdir	掃描子資料夾 (預設值)
– no-subdir	不掃描子資料夾
– max-subdir-level = LEVEL	巢狀子資料夾最多掃描至幾層 (預設值 0 = 無限制)
– symlink	接著捷徑 (預設值)
– no-symlink	略過捷徑

- ext-remove = EXTENSIONS
- ext-exclude = EXTENSIONS　排除以冒號分隔的副檔名不予掃描

方法：

– adware	掃描廣告程式/間諜程式/高風險程式
– no-adware	不掃描廣告程式/間諜程式/高風險程式
– unsafe	掃描有潛在危險的程式
– no-unsafe	不掃描有潛在危險的程式
– unwanted	掃描潛在不需要應用程式
– no-unwanted	不掃描潛在不需要應用程式
– pattern	使用資料庫
– no-pattern	不使用資料庫
– heur	啟用啟發式
– no-heur	停用啟發式
– adv-heur	啟用進階啟發式掃描
– no-adv-heur	停用進階啟發式掃描

清除：

– action = ACTION	對受感染物件執行動作。可用的處理方法：none (無)、clean (清除)、prompt (提示)
– quarantine	將受感染檔案複製到隔離 (補充動作之不足)
– no-quarantine	不將受感染檔案複製到隔離

防護記錄：

– log-file = FILE	將防護記錄輸出到檔案
– log-rewrite	覆寫輸出檔 (預設值 - 附加)
– log-all	也記錄清除檔案
– no-log-all	不記錄清除檔案 (預設值)

掃描的可能結束代碼：

0　- 找不到威脅
1　- 找到威脅但未清除
10　- 仍有部分受感染的檔案
101 - 壓縮檔錯誤
102 - 存取錯誤
103 - 內部錯誤

附註：
若結束代碼大於 100，表示未掃描檔案，檔案可能受感染。

5.4 ESET SysInspector

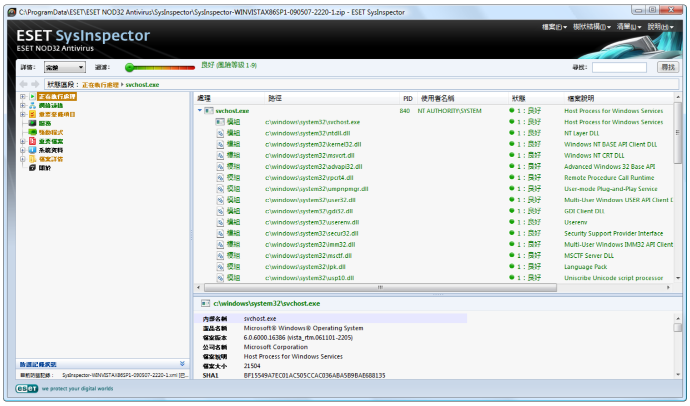
ESET SysInspector 這個應用程式會徹底檢查電腦，並完整地顯示所收集的資料。諸如已安裝驅動程式及應用程式、網路連線或重要登錄項目等資訊，可協助您調查可疑系統行為是肇因於軟體或硬體不相容，還是惡意軟體感染。

在 ESET 系列中，有兩個不同位置可找到 SysInspector。可攜式應用程式(SysInspector.exe)可從 ESET 網站免費下載。另一種存取方式整合於 ESET Smart Security 4 中。若要開啟 SysInspector 區段，請在左下角啟動 [進階] 顯示模式，並按一下 [**工具 > SysInspector**]。兩個方式的功能相同，且具有相同的程式控制項。唯一的差異是管理輸出的方式不同。可攜式應用程式可讓您將系統快照匯出至 XML 檔案，並儲存至您的磁碟。在整合的 SysInspector 中也可執行此操作。此外，您可以方便地將系統快照直接儲存在 [**ESET Smart Security 4** > **工具** > **SysInspector**] 中 (如需相關資訊，請參閱「5.4.1.4 ESS 中的 SysInspector」)。

請留一些時間讓 ESET SysInspector 掃描您的電腦。視硬體配置、作業系統及電腦上安裝的應用程式數量而定，可能需要花費 10 秒到幾分鐘的時間。

5.4.1 使用者介面與應用程式使用

為便於使用，「主視窗」分為四個區段：位於「主視窗」頂端的「程式控制」、位於中間左側的「瀏覽視窗」、位於中間右側的「說明視窗」，以及位於「主視窗」底部右側的「詳細資料視窗」。



5.4.1.1 程式控制

此區段包含 ESET SysInspector 中所有可用程式控制的說明

檔案
您可以按一下這裡，儲存目前的報告狀態以供稍後進行調查，或開啟之前儲存的報告。如果您希望發佈報告，建議您產生適合傳送的報告。此形式的報告會略過機密資訊。

附註：*您只需將之前儲存的 ESET SysInspector 報告拖放至「主視窗」，即會開啟報告。*

樹狀目錄
可讓您展開或關閉所有節點

清單
包含可在程式內更輕鬆瀏覽的功能，以及各類其他功能，例如尋找線上資訊。

重要：*以紅色強調顯示的項目表示未知，所以程式會將它們標記為有潛在的危險性。即使項目是紅色的，也不表示您可以刪除該檔案。刪除之前，請確定檔案確實是危險或不必要的。*

說明
包含應用程式及其功能的相關資訊。

詳細資料
影響「主視窗」其他區段中顯示的資訊，讓程式的使用更加簡單。您可在「基本」模式中，存取用於尋找系統中一般問題解決方案的資訊。在「中等」模式中，程式會顯示較不常用的詳細資料，而在「完整」模式中，ESET SysInspector 會顯示解決專門問題的所有必要資訊。

項目過濾
項目過濾最適用於尋找系統中的可疑檔案或登錄項目。您可使用調整滑桿，根據「風險等級」來過濾項目。如果滑桿設為最左側 (風險等級 1)，則會顯示所有項目。將滑桿移至右側，程式會過濾掉風險小於目前「風險等級」的所有項目，並只顯示超過所顯示層級的可疑項目。滑桿在最右側時，程式只會顯示已知的有害項目。

風險範圍在 6 至 9 的所有項目都會造成安全風險。如果您未使用 ESET 的部分安全性解決方案，建議在程式找到此類項目之後，使用「ESET 線上掃描程式」來掃描系統。「ESET 線上掃描程式」是免費服務，可在 http://www.eset.eu/online-scanner 取得。

附註：*您可比較項目的顏色與「風險等級」滑桿上的顏色，快速判定出項目的「風險等級」。*

搜尋
搜尋可用來根據特定項目的名稱或部分名稱快速尋找該項目。搜尋要求的結果會顯示在 [說明視窗] 中。

返回
按一下向後或向前箭頭，可以返回 [說明視窗] 中之前顯示的資訊。

狀態區段
顯示 [瀏覽視窗] 中的目前節點。

5.4.1.2 瀏覽 ESET SysInspector

ESET SysInspector 會將各類型的資訊分為數個基本區段，稱為節點。您可將每個節點展開至其子節點，瞭解其他詳細資料 (若有的話)。若要開啟或收合節點，只要按兩下節點名稱，或者按一下節點名稱旁邊的 ⊞ 或 ⊟。您可在 [瀏覽視窗] 中瀏覽節點及子節點樹狀結構時，以找到 [說明視窗] 中顯示之每個節點的各類詳細資料。如果您在 [說明視窗] 中瀏覽項目，則每個項目的其他詳細資料會顯示在 [詳細資料視窗] 中。

下列是 [瀏覽視窗] 中主要節點的說明，以及 [說明視窗] 及 [詳細資料視窗] 中的相關資訊。

執行中的處理程序
此節點包含產生報告時執行之應用程式及處理程序的相關資訊。您可以在 [說明視窗] 中，找到每個處理程序的其他詳細資料，例如處理程序使用的動態程式庫及其在系統中的位置、應用程式供應商的名稱、檔案的風險等級等等。

[詳細資料視窗] 包含 [說明視窗] 中所選取項目的其他資訊，例如檔案大小或雜湊。

附註：*作業系統所包含的多數重要核心元件，會全年無休不間斷的執行，並為其他使用者應用程式提供基本與主要功能。在特定情況下，此類處理程序會以 \??\ 開投得檔案路徑，顯示於 ESET SysInspector 工具中。這些符號提供處理程序的啟動前最佳化；對於系統來說是安全且正確的。*

網路連線
[說明視窗] 包含使用 [瀏覽視窗] 中所選取通訊協定 (TCP 或 UDP)、透過網路通訊的處理程序及應用程式清單，以及應用程式連接的遠端位址。您也可以檢查已指定 IP 位址的 DNS 指派情形。

[詳細資料視窗] 包含 [說明視窗] 中所選取項目的其他資訊，例如檔案大小或雜湊。

重要登錄項目
包含所選取登錄項目的清單，通常與各種系統問題相關，例如指定啟動程式、瀏覽器 Helper 物件 (BHO) 等等。

您可在 [說明視窗] 中，找到與特定登錄項目相關的檔案。您可以在 [詳細資料視窗] 中查看其他詳細資料。

服務
[說明視窗] 包含登錄為「Windows 服務」的檔案清單。您可以在 [詳細資料視窗] 中，檢查所設定的服務啟動方式，以及檔案的特定詳細資料。

驅動程式
系統上所安裝的驅動程式清單。

重要檔案
[說明視窗] 會顯示與 Microsoft Window ® 作業系統相關的重要檔案內容。

系統資料
包含硬體及軟體的詳細資訊，以及設定環境變數及使用者權限的相關資訊。

檔案詳情
重要系統檔案及 [Program Files] 資料夾中檔案的清單。您可在 [說明視窗] 及 [詳細資料視窗] 中找到檔案的其他特定資訊。

關於
ESET SysInspector 的相關資訊

5.4.1.3 比較

[比較] 功能可讓使用者比較兩個現有防護記錄。此功能會比較出兩個防護記錄中不相符的項目。如果您想要追蹤系統中的變更，則適用此功能，例如，可用來偵測惡意代碼的活動。

啟動之後，應用程式會建立新的防護記錄並顯示在新視窗中。瀏覽至 [**檔案 -> 儲存防護記錄**]，將防護記錄儲存為檔案。您可以稍後開啟並檢視防護記錄檔案。若要開啟現有防護記錄，請使用 [**檔案 -> 開啟防護記錄**] 功能表。在主要程式視窗中，ESET SysInspector 每次僅顯示一個防護記錄。

如果您比較兩個防護記錄，則原則是將目前作用中的防護記錄與已儲存在檔案中的防護記錄進行比對。若要比較防護記錄，請使用 [**檔案 -> 比較防護記錄**] 選項，並選擇 [**選取檔案**]。所選防護記錄會與主要程式視窗中的作用中防護記錄進行比較。產生的結果稱為比較防護記錄，只會顯示這兩個防護記錄之間的差異。

附註：*若您比較兩個防護記錄檔案、選取 [檔案 -> 儲存防護記錄]，並將其儲存為 ZIP 檔案，則兩個檔案都會儲存。稍後開啟此類檔案時，則會自動比較包含的防護記錄。*

SysInspector 會所顯示項目的旁，以符號識別所比較防護記錄之間的差異。標記為 − 的項目只能在作用中的防護記錄中找到，並不存在於開啟的比較防護記錄中。而標記為 + 的項目只能在開啟的防護記錄中找到，並不存在於作用中防護記錄。

項目旁所顯示的所有符號說明：

+ 新值，不存在於上一個防護記錄中

⊞ 樹狀結構區段包含新值

− 已移除的值，只存在於上一個防護記錄中

⊟ 樹狀結構區段包含已移除的值

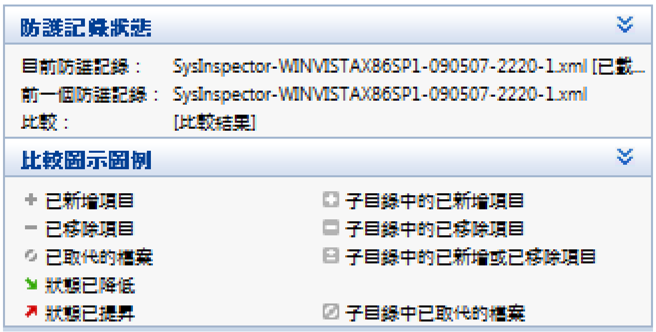
值/檔案已變更

樹狀結構區段包含已修改的值/檔案

風險等級已降低 / 在上一個防護記錄中較高

風險等級已增加 / 在上一個防護記錄中較低

左下角顯示的說明區段會說明所有符號，並顯示進行比較的防護記錄名稱。



所有的比較防護記錄都可以儲存至檔案，並在稍後開啟。

範例：
產生記錄系統原始資訊的防護記錄，並將其儲存為 previous.xml。在變更系統之後，開啟 SysInspector 並讓其產生新的防護記錄。將其儲存至名為 current.xml 的檔案。

若要追蹤這兩個防護記錄之間的變更，請瀏覽至 [**檔案 -> 比較防護記錄**]。程式會建立比較防護記錄，顯示防護記錄之間的差異。

如果使用下列指令列選項，也可達到相同的結果：

SysIsnpector.exe current.xml previous.xml

5.4.1.4 ESET Smart Security 4 中的 SysInspector

若要在 ESET Smart Security 4 中開啟 SysInspector 區段，請按一下 [**工具** > **SysInspector**]。SysInspector 視窗中的管理系統與電腦掃描防護記錄或排定工作的管理系統類似。所有使用系統快照的作業 (建立、檢視、比較、移除及匯出) 都可透過按一或兩下進行存取。

[SysInspector] 視窗包含所建立快照的基本資訊，例如建立時間、簡短註解，建立快照的使用者名稱及快照狀態。

若要 [**比較**]、[**新增...**] 或 [**移除**] 快照，請使用位於 SysInspector 視窗中快照清單下方的對應按鈕。亦可從內容功能表中使用這些選項。若要檢視選取的系統快照，請使用 [**檢視**] 內容功能表選項。若要將選取的快照匯出為檔案，請在該快照上按一下滑鼠右鍵，並選取 [**匯出...**]。下列是可用選項的詳細說明：

比較 – 可讓您比較兩個現有防護記錄。如果您想要追蹤目前防護記錄與較舊防護記錄之間的變更，即適用此選項。您必須選取要比較的兩個快照，此選項才會生效。

新增 – 建立新記錄。您必須先輸入關於記錄的簡短註解，才能新增記錄。若要找到 (目前已產生快照的) 快照建立進度百分比，請參閱 [狀態] 直欄。所有已完成快照都會標記為 [已建立] 狀態。

移除 – 從清單中移除項目

顯示 – 顯示選取的快照。或按兩下所選項目，亦有相同效果。

匯出... – 將選取的項目儲存為 XML 檔案 (同時儲存為壓縮版本)

5.5 ESET SysRescue

ESET Recovery CD (ERCD) 是一個公用程式，可讓您建立包含 ESET Smart Security 4 (ESS) 的開機磁碟。ESET Recovery CD 的主要優點是 ESS 的執行不受限於主機作業系統，且同時可以直接存取磁碟及整個檔案系統。也因為這樣，所以能夠移除平常 (如作業系統執行過程中) 無法移除的入侵。

5.5.1 最低需求

ESET SysRescue (ESR) 的運作環境為以 Windows Vista 為基礎的「Microsoft Windows 預先安裝環境 (Windows PE)」2.x 版。Windows PE 是免費套件 Windows Automated Installation Kit (Windows AIK) 的一部分，因此必須先安裝 Windows AIK 才能建立 ESR。因為支援 32 位元版本的 Windows PE，所以 ESR 只能在 32 位元版本的 ESS/ENA 中建立。ESR 支援 Windows AIK 1.1 及更新版本。ESR 包含於 ESS/ENA 4.0 及更高版本中。

5.5.2 如何建立救援 CD

如果符合建立 ESET SysRescue (ESR) CD 的最低需求，則可輕易地完成此工作。若要啟動 ESR 精靈，請按一下 [**開始** > **程式集** > **ESET** > **ESET Smart Security 4** > **ESET SysRescue**]。

首先，精靈會檢查是否有 Windows AIK 與適用於建立開機媒體的裝置。

接著會選取要放置 ESR 的目標媒體。除了 CD/DVD/USB 之外，您也可以選擇將 ESR 儲存在 ISO 檔案中。稍後，您可以將 ISO 映像燒錄在 CD/DVD 中，或以其他方式 (例如，在 VmWare 或 Virtualbox 等虛擬環境中) 使用。

指定所有參數之後，您會在 ESET SysRescue 精靈的最後一個步驟中，看到編譯預覽。檢查參數並開始編譯。可用的選項包括：

資料夾
ESET Antivirus
進階
可開機 USB 裝置
燒錄

5.5.2.1 資料夾

暫存資料夾是 ESET SysRescue 編譯期間所需檔案的工作目錄。

ISO 資料夾是編譯完成之後，儲存所產生 ISO 檔案的資料夾。

此索引標籤上的清單顯示所有本機及對應的網路磁碟機，以及可用空間。若其中部分資料夾所在磁碟機的可用空間不足，建議您選取其他具有更多可用空間的磁碟機。否則，編譯可能會因可用磁碟空間不足而提前結束。

外部應用程式
可讓您指定會在 SysRescue 媒體開機之後執行或安裝的其他程式。

併入外部應用程式 – 可將外部程式新增至 SysRescue 編譯

選取的資料夾 – 要新增至 SysRescue 磁碟之程式所在的資料夾

5.5.2.2 ESET 病毒防護

若要建立 ESET SysRescue CD，您可以選取兩種 ESET 檔案來源，供編譯器使用。

ESS 資料夾 – 已安裝 ESET 產品的電腦上，安裝資料夾中包含的檔案

MSI 檔案 – 使用 MSI 安裝程式中包含的檔案

設定檔 – 您可以使用下列兩個使用者名稱及密碼來源的其中一個：

已安裝 ESS – 從目前安裝的 ESET Smart Security 4 或 ESET NOD32 複製使用者名稱及密碼

來源使用者 - 使用輸入於下方對應文字方塊中的使用者名稱及密碼

附註：*ESET SysRescue CD 中的 ESET Smart Security 4 或 ESET NOD32 Antivirus 會從網際網路更新，或從執行 ESET SysRescue CD 之電腦上所安裝的 ESET Security 解決方案更新。*

5.5.2.3 進階

[**進階**] 索引標籤可讓您針對電腦記憶體的大小，對 ESET SysRescue CD 進行最佳化。選取 [**512 MB 及以上**]，將 CD 的內容寫入作業記憶體 (RAM)。如果您選取 [**少於 512 MB**]，則執行 WinPE 時會永久存取復原 CD。

外部磁碟機 – 您可在此區段中插入特定硬體 (通常為網路介面卡) 的驅動程式。雖然 WinPE 的基礎 (Windows Vista SP1) 可支援廣泛的硬體，但有時還是無法識別硬體，必須手動新增驅動程式。您可使用下列兩種方式，將驅動程式引進 ESET SysRescue 編譯：手動 ([**新增**] 按鈕) 及自動 ([**自動搜尋**] 按鈕)。若是手動引進，請選取對應 .inf 檔案的路徑 (此資料夾中還必須具有適用的 *.sys 檔案)。若是自動引進，則會在所提供的電腦作業系統中，自動找到驅動程式。建議只有當使用 SysRescue 的電腦與建立 SysRescue 的電腦使用相同的網路介面卡時，才使用自動引進。建立 ESET SysRescue 期間，會將驅動程式引進編譯，讓使用者無須稍後個別尋找。

5.5.2.4 可開機 USB 裝置

如果您已選取 USB 裝置作為目標媒體，則可以在 [可開機 USB 裝置] 索引標籤上選取一個可用 USB 媒體 (如果有多個 USB 裝置的話)。

警告：*選取的 USB 裝置會在建立 ESET SysRescue 的處理程序期間進行格式化，也就是說，裝置上的所有資料都會被刪除。*

5.5.2.5 燒錄

如果您選取 CD/DVD 作為目標媒體，則可以在 [燒錄] 索引標籤上指定其他燒錄參數。

刪除 ISO 檔案 – 勾選此選項，在建立「ESET 救援 CD」之後刪除 ISO 檔案。

已啟用刪除 - 可讓您選取快速消除及完全消除。

燒錄裝置 - 選取要用來燒錄的磁碟機。

警告：*這是預設選項。如果使用可重新寫入 CD/DVD，則會消除所有包含的資料。*

[媒體] 區段包含目前插入 CD/DVD 裝置之媒體的相關資訊。

燒錄速度 – 從下拉式功能表中選取想要的速度。選取燒錄速度時，應考量燒錄裝置的容量及使用的 CD/DVD 類型。

5.5.3 使用 ESET SysRescue

為能有效地使用救援 CD/DVD/USB，請讓電腦可從 ESET SysRescue 開機媒體開機。您可在 BIOS 中修改開機優先順序。或可以在電腦啟動期間呼叫開機功能表 - 通常使用 F9 - F12 鍵的其中一個，需視主機板/BIOS 的版本而定。

開機之後就會啟動 ESS/ENA。因為 ESET SysRescue 只能在特定情況下使用，所以不需要使用平常在 ESS/ENA 中的部分保護模組及程式功能；其清單縮小為 [電腦掃描]、[更新] 及 [設定] 中的部分區段。ESET SysRescue 最重要的功能就是能夠更新病毒資料庫。建議您在啟動［電腦掃描］之前，先更新程式。

5.5.3.1 使用 ESET SysRescue

假設網路中的電腦已感染可修改執行檔（EXE）的病毒。ESS/ENA 能夠清除所有受感染的檔案，但 explorer.exe 除外，即使在「安全」模式中也無法清除。

這是由於 explorer.exe 為必要的 Windows 處理程序之一，即使在「安全模式」中也會啟動。ESS/ENA 不能對該檔案執行任何處理方法，因此它仍會保持感染狀態。

在這樣的情況中，請使用 ESET SysRescue 來解決問題。ESET SysRescue 不需要主機作業系統中的任何元件。因此能夠處理（清除、刪除）磁碟中的任何檔案。

6. 詞彙

6.1 入侵類型

「入侵」是嘗試進入及/或損害使用者電腦的一種惡意軟體。

6.1.1 病毒

電腦病毒是會損毀電腦上現有檔案的入侵活動。病毒這個名稱取自生物學的病毒，因為它會利用類似的方式，從一部電腦散播至另一部電腦。

電腦病毒主要會攻擊執行檔及文件。為進行複製，病毒會將其「內容」附加在目標檔案結尾。簡而言之，電腦病毒的運作如下：執行受感染的檔案之後，病毒會 (在原始應用程式之前) 自行活化，並執行其預先定義的工作。之後才會讓原始應用程式執行。除非使用者自己 (有意或無意) 執行或開啟惡意程式，否則病毒無法感染電腦。

電腦病毒的活動力與嚴重性各異。有些病毒會故意將硬碟機中的檔案刪除，因而極度危險。但有些病毒並不會造成真正的損害，而只會困擾使用者，以展現作者的技術。

有一點要特別注意的是，病毒 (與特洛伊木馬程式或間諜程式相較) 慢慢地愈來愈少見，因為對惡意軟體的作者而言，它們沒有什麼商業誘因。此外，「病毒」這個詞經常被誤用來泛指各種入侵活動。目前，這種情況已逐漸減少，而改用較精確的新詞彙「惡意軟體」。

如果您的電腦感染病毒，則必須將被感染的檔案還原為原來的狀態，也就是使用防毒程式來清除病毒。

病毒的範例如下：OneHalf、Tenga 及 Yankee Doodle。

6.1.2 蠕蟲

電腦蠕蟲是含有惡意程式碼的程式，它會攻擊主機電腦，並透過網路散佈。病毒與蠕蟲的基本差異在於，蠕蟲能夠自行複製及傳輸。蠕蟲不需仰賴主機檔案 (或開機磁區)。

蠕蟲會透過電子郵件或網路封包等方式來擴散。就此而言，蠕蟲可以用二種方式分類：

- **電子郵件** – 自行散佈至在使用者通訊錄中找到的電子郵件地址，以及
- **網路** – 利用各種應用程式中的安全性弱點。

因此，蠕蟲的存活率比電腦病毒高出許多。因為網際網路的普及，蠕蟲可能在發佈的數小時內，就散佈到全世界，有時甚至只需幾分鐘的時間。這種獨立又快速的複製能力，使它比其他類型的惡意軟體 (例如病毒) 更加危險。

在系統中活化的蠕蟲會造成許多不便：如刪除檔案、降低系統效能，甚至會停用某些程式。電腦蠕蟲的本質使它能夠成為其他入侵類型的「傳輸媒介」。

如果您的電腦感染了電腦蠕蟲，我們建議您刪除受感染的檔案，因為其中可能包含惡意代碼。

知名的蠕蟲範例如下：Lovsan/Blaster、Stration/Warezov、Bagle 及 Netsky。

6.1.3 特洛伊木馬程式

從歷史角度來看，電腦特洛伊木馬程式已被定義為一種入侵活動類別，它會嘗試以有用的程式呈現，矇騙使用者執行這些程式。但請注意，對特洛伊木馬程式來說，自古以來事實就是如此，它已經不需要再偽裝自己。它唯一的目的，就是用最容易的方法進行入侵，並達成其惡意的目標。「特洛伊木馬程式」已經變成非常普遍的詞彙，用以描述無法歸入特定類別的入侵。

由於這是非常廣泛的類別，所以通常會細分為許多子類別。最廣為人知的類別如下：

- downloader – 會從網際網路下載其他入侵的一種惡意程式。
- dropper – 這種特洛伊木馬程式類型主要會將其他類型的惡意軟體放置在被入侵的電腦上。
- backdoor – 一種與遠端攻擊者通訊的應用程式，可讓攻擊者存取系統，進而控制系統。
- keylogger – (按鍵側錄程式) - 此程式會記錄使用者按下的每一個按鍵，並將該資訊傳送給遠端攻擊者。
- dialer – dialer 是專門用來連線至高費率電話號碼的程式。使用者幾乎不可能查覺到建立了新連線。Dialer 只能對使用撥接數據機的使用者造成損害，而現在已經不常使用撥接數據機了。

特洛伊木馬程式通常採用副檔名為 .exe 的執行檔形式。如果偵測到您的電腦上有某個檔案是特洛伊木馬程式，建議您將它刪除，因為其中極可能包含惡意代碼。

知名的特洛伊木馬程式範例如下：NetBus、Trojandownloader.Small.ZL、Slapper

6.1.4 Rootkit

Rootkit 是惡意程式，可讓網際網路攻擊者神不知鬼不覺的任意存取系統。Rootkit 在存取系統之後 (通常是利用系統弱點)，會使用作業系統中的功能來躲避防毒軟體的偵測：它會隱藏處理程序、檔案及 Windows 登錄資料。因此，使用一般的測試技術幾乎不可能偵測得到。

在談到 Rootkit 防護時，請記得偵測可分為二種等級：

1. 當其嘗試存取系統時。Rootkit 尚未存在，所以沒有作用。大部分的防毒系統都能夠在此層級消滅 Rootkit (假設系統真的偵測到這些檔案被感染)。
2. 當 Rootkit 躲過一般測試時。ESET 防毒系統的使用者擁有「反隱藏」技術的優勢，亦可偵測及消滅作用中的 Rookit。

6.1.5 廣告程式

廣告程式是廣告支援軟體的簡稱。舉凡可顯示廣告資料的程式均屬於這個種類的軟體。廣告程式應用程式會經常在網際網路瀏覽器中自動開啟包含廣告的快顯視窗，或變更瀏覽器的首頁。廣告程式通常隨附於免費軟體程式，讓其建立者得以負擔其 (通常很實用) 應用程式的開發成本。

廣告程式本身並不危險 – 只是使用者會受到廣告的騷擾。其危險性在於廣告程式可能也會執行追蹤功能 (如同間諜程式的功能)。

如果您決定使用免費軟體產品，請特別注意安裝程式。安裝程式很可能會在安裝額外廣告程式程式時通知您。您通常可以取消安裝廣告程式，只安裝程式。但有些情況是，不安裝廣告程式便無法安裝部分程式，或者會限制程式的功能。這表示廣告程式能以「合法」方式存取系統，因為使用者已同意。在此情況下，保證安全總比留下遺憾好。

如果在您的電腦上偵測到某個檔案是廣告程式，則建議您將其刪除，因為其中極可能包含惡意代碼。

6.1.6 間諜程式

此類別包括會在使用者未同意/不知情的情況下，傳送私人資訊的所有應用程式。它們會利用追蹤功能來傳送各種統計資料，例如：造訪過的網站清單、使用者通訊錄中的電子郵件地址，或是輸入過的按鍵清單。

間諜程式的作者會宣稱這些技術的目的是為了深入瞭解使用者的需求及興趣，使宣傳目標更為精準。問題是有益與惡意的應用程式之間沒有明顯的分界，而且沒有人可以確保所擷取的資訊不會被濫用。間諜應用程式取得的資料可能包含安全密碼、PIN、銀行帳號等等。免費版程式的作者通常會將間諜程式搭載於該程式，以創造收益，或是激勵您購買軟體。通常在程式安裝期間，就會讓使用者知道間諜程式的存在，以刺激其升級為沒有間諜程式的付費版本。

例如，P2P (點對點) 網路的用戶端應用程式，搭載間諜程式的免費軟體產品之著名範例。Spyfalcon 或 Spy Sheriff (以及許多其他程式) 是屬於特定的間諜程式子類別 – 看似反間諜程式，但事實上本身就是間諜程式。

如果在您的電腦上偵測到某個檔案是間諜程式，建議您將它刪除，因為其中極可能包含惡意程式碼。

6.1.7 有潛在危險的程式

有很多合法程式都可用來簡化網路電腦的系統管理作業。然而，如果落入壞人手中，可能就會被用來從事惡意活動。這就是 ESET 要建立這個特殊類別的原因。我們的客戶可以選擇防毒系統是否要偵測這類威脅。

「有潛在危險的程式」是用於商業、合法軟體的分類。此分類包括的程式諸如遠端存取工具、密碼破解應用程式，以及 keylogger (會記錄使用者所按按鍵的程式)。

若您在電腦上發現有潛在危險的程式，是您未曾安裝但卻執行中的，請洽詢您的網路系統管理員，或是移除該應用程式。

6.1.8 潛在不需要應用程式

潛在不需要應用程式不一定是惡意的，但是對電腦效能可能會造成負面影響。這些應用程式通常需要經過同意才能安裝。如果您的電腦上有這類應用程式，系統的表現會與安裝這類應用程式之前有所不同。最顯著的變更如下：

- 開啟您從未看過的新視窗
- 啟動並執行隱藏的處理程序
- 系統資源的用量增加
- 搜尋結果變更
- 應用程式會與遠端伺服器通訊

6.2 遠端攻擊的類型

有很多特殊的技術可讓攻擊者危害遠端系統。這些技術可分為數種類別。

6.2.1 DoS 攻擊

DoS 或「拒絕服務」是嘗試使目標使用者無法使用電腦或網路的方式。受影響之使用者間的通訊會到受阻礙，並且無法再繼續正常運作。遭受 DoS 攻擊的電腦通常需要重新啟動，才能正常運作。

在大部分的情況下，攻擊目標是 Web 伺服器，而攻擊目的是讓使用者在某段時間內無法使用。

6.2.2 DNS Poisoning

駭客可以透過 DNS (網域名稱伺服器) Poisoning 方法，欺騙所有電腦的 DNS 伺服器，讓其相信提供的假資料是合法且可信的。然後，會在某段時間內快取假資訊，讓攻擊者可以重新寫入 IP 位址的 DNS 回應。因此，嘗試存取網際網路站台的使用者會下載到電腦病毒或蠕蟲，而不會下載到原始內容。

6.2.3 蠕蟲攻擊

電腦蠕蟲是含有惡意程式碼的程式，它會攻擊主機電腦，並透過網路散佈。網路蠕蟲會利用各種應用程式中的安全性弱點。因為網際網路的普及，蠕蟲可能在發佈的數小時內，就散佈到全世界。有時甚至只需幾分鐘的時間。

使用防火牆中的預設安全性設定，或是封鎖未受保護及未使用的通訊埠，即可避免大部分的蠕蟲攻擊 (Sasser、SqlSlammer)。此外，亦請務必以最新的安全修補程式來更新作業系統。

6.2.4 通訊埠掃描

連接埠掃描可控制網路主機上是否有開放式電腦連接埠。連接埠掃描器就是為了尋找這類連接埠而設計的軟體。

電腦連接埠是虛擬端點，可處理對內及對外的資料 – 就安全角度而言非常重要。在大型網路中，通訊埠掃描器所收集的資訊有助於識別潛在的弱點。這種用法是合法的。

儘管如此，通訊埠掃描還是經常被駭客用來嘗試破壞安全性。第一步就是傳送封包至每一個通訊埠。依據回應類型，可以判斷出哪些通訊埠在使用中。掃描作業本身並不會造成損害，但請注意這種活動會顯露出潛在的弱點，而讓攻擊者有機會操控遠端電腦。

建議網路系統管理員封鎖所有未使用的通訊埠，並保護使用中的通訊埠不受未經授權的存取。

6.2.5 TCP 去同步化

TCP 去同步化是 TCP 劫持攻擊中所使用的技術。當對內封包中的序號與預期的序號不同時，就會觸發此技術。含非預期序號的封包會被丟棄 (如果是出現在目前的通訊視窗中，則會儲存在緩衝存放區)。

在去同步化的狀態中，二邊的通訊端點都會丟棄所接收的封包。遠端攻擊者就會趁這個時候入侵，並提供封包正確的序號。攻擊者甚至可以透過指令來操控通訊，或是用其他方式修改。

TCP 劫持攻擊的目的是要中斷伺服器對用戶端或點對點通訊。在每個 TCP 區段上使用驗證，可以避免許多攻擊。另外，也建議您在網路裝置上使用建議配置。

6.2.6 SMB Relay

SMBRelay 及 SMBRelay2 是特殊的程式，可對遠端電腦發動攻擊。這二種程式會利用伺服器訊息區檔案共用通訊協定 (上至 NetBIOS 層級)。如果使用者在 LAN 中共用任何資料夾或目錄，就極可能使用此檔案共用通訊協定。

在區域網路通訊中，會交換密碼雜湊。

SMBRelay 會在 UDP 通訊埠 139 及 445 上接收連線，轉送用戶端和伺服器交換的封包，再加以修改。連線並驗證之後，即中斷用戶端的連線。SMBRelay 會建立新的虛擬 IP 位址。使用 net use \\192.168.1.1 指令即可存取新位址。接著所有 Windows 網路功能都可以使用該位址。SMBRelay 會轉送 SMB 通訊協定通訊，但交涉及驗證除外。用戶端電腦一經連線，遠端攻擊者即可使用該 IP 位址。

SMBRelay2 作用的原理與 SMBRelay 相同，只是它是使用 NetBIOS 名稱，而不是 IP 位址。這二種程式都會執行「中間人」(man-in-the-middle) 攻擊。這些攻擊可讓遠端攻擊者讀取、插入及修改在二個通訊端點之間交換的郵件，而不被發現。暴露在這種攻擊下的電腦常會停止回應或突然重新啟動。

為避免這些攻擊，建議您使用驗證密碼或金鑰。

6.2.7 ICMP 攻擊

ICMP (網際網路控制訊息通訊協定) 是一種普及且廣泛使用的網際網路通訊協定。它主要由連線電腦用於傳送各種錯誤訊息。

遠端攻擊者嘗試利用 ICMP 通訊協定的弱點。ICMP 通訊協定設計用來進行不需要驗證的單向通訊。這樣可讓遠端攻擊者觸發所謂的 DoS (拒絕服務) 攻擊，或者授與未獲授權的個人對內與對外封包的存取權。

ICMP 攻擊的典型範例是：Ping Flood、ICMP_ECHO Flood 及 Smurf 攻擊。遭受 ICMP 攻擊的電腦明顯變慢 (這適用於使用網際網路的所有應用程式)，而且連接到網際網路時會發生問題。

6.3 電子郵件

電子郵件是一種具有很多優點的現代通訊形式。其靈活、快速且直接。在 20 世紀早期，電子郵件在網際網路的擴散中扮演關鍵的角色。

很遺憾，由於具有高度的匿名性，電子郵件及網際網路也為垃圾郵件之類的非法活動創造了空間。廣義上分類，垃圾郵件包括來路不明的廣告、惡意軟體 (即惡意程式) 的欺騙及擴散。傳送的成本接近於零的事實會增加使用者的不便及危險，而且垃圾郵件的作者擁有許多工具及來源可用於取得新的電子郵件位址。此外，垃圾郵件容量及多樣性使得管理更加困難。您使用電子郵件位址的時間越長，其最後變成垃圾郵件引擎資料庫的可能性就越高。預防的某些提示：

- 可能的話，請勿在網際網路上發佈您的電子郵件位址
- 僅將您的電子郵件位址提供給信任的個人
- 可能的話，請勿使用一般別名，因為別名越複雜，追蹤的可能性越低
- 請勿回覆已到達收件匣中的垃圾郵件
- 填寫網際網路表單時請小心，並特別注意「是，我想要在我的收件匣中接收... 的相關資訊。」之類的核取方塊。
- 請使用「專門的」電子郵件位址，例如，一個位址用於工作，另一個位址用於與您的朋友通訊等。
- 時常變更您的電子郵件位址
- 使用防毒解決方案

6.3.1 廣告

網際網路廣告是增長最為迅速的廣告形式之一。電子郵件被當作廣告的媒介。其主要的行銷優勢在於零成本、高直接性及有效性；而且，訊息幾乎是立即傳遞的。許多公司都使用電子郵件行銷工具來與目前及潛在客戶進行有效的溝通。

由於使用者可能願意接收某些產品的商業資訊，所以這種廣告方式是合法的。但事實上，很多公司會傳送來路不明的大量商業訊息。在這種情況下，電子郵件廣告就會變成垃圾郵件。

大量來路不明的商業電子郵件已成為真實的問題，因為它沒有任何減少的跡象。來路不明電子郵件的作者會嘗試將垃圾郵件偽裝成合法郵件。另一方面，大量合法廣告可能會導致負面的反應。

6.3.2 惡作劇

惡作劇是透過網際網路擴散的一種訊息。這種訊息通常透過電子郵件傳送，有時透過通訊工具 (如 ICQ 及 Skype) 傳送。通常訊息本身是惡作劇或「都市傳奇」。

「電腦病毒」惡作劇會嘗試在收件者中產生恐懼、不確定及懷疑 (FUD)，讓他們相信存在「無法偵測的病毒」正在刪除檔案並擷取密碼，或者在其電腦上執行部分其他有害活動。

部分惡作劇的目的在於對他人造成情感上的困惑。收件者會被要求將此類訊息傳送至其所有連絡人，這使惡作劇循環不息。還有行動電話惡作劇，尋求協助，有人從海外向您提供金錢等。大部分情況下，無法追蹤建立者的意圖。

大體上，如果您看到一則訊息提示您將其傳遞給您認識的每個人，則它很可能是惡作劇。網際網路上有許多特定網站，可以驗證電子郵件是否合法。傳送之前，對您懷疑是惡作劇的訊息執行網際網路搜尋。

6.3.3 網路釣魚

網路釣魚這個詞彙是用來定義利用社交工程技巧 (操縱使用者以取得機密資訊) 的犯罪活動。其目的是要存取像是銀行帳號、PIN 碼等敏感資料。

攻擊者通常會假冒成值得信賴的個人或企業（金融機構、保險公司）來傳送電子郵件，以進行存取。該電子郵件看起來非常逼真，而且會包含源自其模仿對象的圖片及內容。它會以各種藉口（資料驗證、金融作業）要求您輸入您的個人資料，即銀行帳號或使用者名稱及密碼。這類資料一經提交，就很容易被竊取及濫用。

請注意，銀行、保險公司及其他合法公司絕不會以來路不明的電子郵件，主動要求使用者名稱及密碼。

6.3.4 識別垃圾郵件詐騙

一般而言，有幾個指標可協助您識別信箱中的垃圾郵件 (來路不明的電子郵件)。如果郵件至少滿足下列某些條件，則它極可能是垃圾郵件。

- 寄件者位址不屬於連絡人清單中的某人
- 向您提供一大筆金錢，但是您必須先提供少數金額
- 以各種借口 (資料驗證、金融作業) 要求您輸入某些個人資料：銀行帳戶號碼、使用者名稱及密碼等。
- 以外文撰寫
- 要求您購買不感興趣的產品。如果您仍然決定購買，請驗證郵件寄件者是可靠的廠商 (洽詢原始產品製造商)。
- 拼錯某些單字，以嘗試欺騙您的垃圾郵件過濾器。例如 vaigra 而不是 viagra 等。

6.3.4.1 規則

在「垃圾郵件防護」解決方案及電子郵件用戶端的內容中，規則是用來操作電子郵件功能的工具。其分為二個邏輯部分：

1. 條件 (例如，從特定位址對內的郵件)
2. 處理方法 (例如，刪除郵件、將郵件移至指定的資料夾)。

規則的數量及組合會依「垃圾郵件防護」解決方案而有所不同。這些規則是做為對付垃圾郵件 (來路不明的電子郵件) 的措施。典型範例：

- 1. 條件：對內的電子郵件中包含通常會在垃圾郵件中看到的某些字眼
  2. 處理方法：刪除郵件
- 1. 條件：對內的電子郵件中包含副檔名為 .exe 的附件
  2. 處理方法：刪除附件，並傳送郵件至信箱
- 1. 條件：對內的郵件是來自您的雇主
  2. 處理方法：將郵件移至 [工作] 資料夾。

建議您使用「垃圾郵件防護」程式中的規則組合，以方便管理，並提升過濾垃圾郵件 (來路不明的電子郵件) 的效率。

6.3.4.2 貝氏過濾

貝氏垃圾郵件過濾是一種很有效的電子郵件過濾形式，幾乎所有「垃圾郵件防護」產品均可使用。它能夠以較高的準確度識別來路不明的電子郵件。貝氏過濾能夠根據個別使用者的需求為基礎進行運作。

其功能係以下列原則為基礎：第一階段為「學習」處理程序。使用者手動將足夠數量的訊息標記為合法郵件或垃圾郵件 (通常為 200/200)。過濾器會同時分析兩種類別，並瞭解譬如垃圾郵件通常包含 rolex 或 viagra 等單字，而合法郵件是由家庭成員傳送，或從使用者連絡人名單中的位址傳送。如果已處理大量郵件，貝氏過濾就可以將特定「垃圾郵件索引」指派給每封郵件，以判斷其是否為垃圾郵件。

「靈活性」是此功能的主要優點。比方說，如果使用者是生物學家，則有關生物學或相關研究領域的所有對內電子郵件通常會收到較低的可能性索引。如果郵件中含有會將其限定為來路不明郵件的單字，但該郵件是由連絡人名單中的某人所傳送的，則會其將標記為合法，因為連絡人名單中的寄件者會降低垃圾郵件的整體可能性。

6.3.4.3 白名單

一般而言，白名單是被接受或被授與存取權的項目或人員清單。「電子郵件白名單」這個詞是定義使用者想要接收之郵件寄件者的連絡人名單。這種白名單的依據是在電子郵件位址、網域名稱或 IP 位址中搜尋到的關鍵字。

如果白名單是以「排外模式」執行，則不會接收來自任何其他位址、網域或 IP 位址的郵件。另一方面，若非排外模式，則不會刪除這類郵件，但會以其他方式進行過濾。

白名單所依據的原則與黑名單相反。與黑名單相較，白名單相對較容易維護。建議您並用「白名單」與「黑名單」，以提升過濾垃圾郵件的效率。

6.3.4.4 黑名單

通常，黑名單是無法接受或遭到禁止之項目或人員的清單。在虛擬世界中，該技術可讓使用者接受所有來自此清單外之使用者的郵件。

黑名單的形式有兩種。使用者可以在其「垃圾郵件防護」程式中建立自己的黑名單。亦可在網際網路上也可以找到由專門機構建立之定期更新的黑名單。

「黑名單」所依據的原則與白名單相反。黑名單是順利封鎖垃圾郵件的必備要素，但是由於每天都有要封鎖的新項目出現，因此很難進行維護。我們建議您同時使用「白名單」與「黑名單」，以更有效地過濾垃圾郵件。

6.3.4.5 伺服器端控制

伺服器端控制是一種可利用已接收的郵件數目及使用者反應為基礎，來識別大量垃圾郵件的技術。根據郵件的內容，每封郵件都會在伺服器上留下唯一的數位「蹤跡」。事實上，這是唯一的 ID 號碼，並且無法敘述電子郵件的任何內容。兩封完全相同的郵件將會有完全相同的蹤跡，而不同的郵件會有不同的蹤跡。

如果將郵件標記為垃圾郵件，則其蹤跡會傳送至伺服器。如果伺服器接收到更多 (與某垃圾郵件相對應的) 相同蹤跡，就會將該蹤跡儲存在垃圾郵件蹤跡資料庫中。掃描對內的郵件時，程式會將郵件的蹤跡傳送至伺服器。對於經使用者標記為垃圾郵件之郵件，伺服器會傳回與其對應之蹤跡的相關資訊。